Reserve Component Automation Systems (RCAS)

Continuity of Operations Plan (COOP)

for the

Advanced Information Technology Systems (AITS) Task Order

AITS-COOP-U-R7C8
CDRL 5-007

31 May 2012

Prepared for:

UNITED STATES ARMY PROGRAM EXECUTIVE OFFICE ENTERPRISE INFORMATION SYSTEMS (USA PEO EIS)

Prepared by:

Science Applications International Corporation
AITS Operation
6565 Arlington Blvd.
Falls Church, VA 22042

Revision History

Rev.	Date	Description of Change
R0C0	11 November 2008	Initial Submission
R1C0	30 January 2009	Quarterly Update
R2C0	30 April 2009	Quarterly Update
R3C0	30 July 2009	Quarterly Update
R3C1	15 September 2009	Document addresses multiple Government comments that were received on 24 August 2009.
R4C0	30 October 2009	Quarterly Update and inclusion of responses to Government comments received on 14 October 2009
R5C0	29 January 2010	Quarterly Update with changes to • Pg. iv – updated distribution list. • Pg. 3 – updated PRIME INTEGRATOR organizational chart to include Joon Chang as Enterprise Test Manager • Pg. D2 – updated PRIME INTEGRATOR Facility Manager to reflect Jeffrey Montgomery instead of Barbara Neff

Rev.	Date	Description of Change
R6C0	26 April 2010	Quarterly update to address PEO EIS Information Assurance Program Manager (IAPM) visit 17 MAR 10 – changes to: • Section 10 pg 25 added a paragraph and bullets to address additional training requirements • Section 12 pg 28 changed Appendix C to Sample Annual COOP Test Checklist and changed other Appendix letters appropriately • Appendix C pg C-2 added new annual test checklist • Appendix E pg E-5 and E-6 updated Rita Bartholomew and Mitchell Champney's title and contact information • Section 10 pg 25 and 26 added new content to reflect needs of the Sample Annual COOP Test Checklist (Appendix C) • Changed pg vi Section 13 Document Organization to Section 12 Document Organization

Rev.	Date	Description of Change
R7C0	28 May 2010	COOP document has been rewritten in accordance direction provided by the PD RCAS in contract modification delivered 18 March 2010. Document contents, layout, and appendices have been changed to reflect new direction of the COOP
…R7C1	9 July 2010	COOP document updated to incorporate comments received by Government 21 June 2010 in regards to document R7C0
R7C2	20 August 2010	COOP document updated to incorporate comments received by Government in regards to document R7C1. Also updated were the following items: • Table 3 pg. C-2 updated Justin Bragg's office phone number. • Section F.6 pg. F-2 updated 2nd bullet under "Notification Roster" to reflect full "enosc_watch" e-mail address.

Rev.	Date	Description of Change
R7C3	23 September 2010	COOP document updated to incorporate comments received by Government in regards to document R7C2. Also updated were the following items: Table 5, pg C-1 updated office locations. Table 7, pg C-3 updated office locations. Appendix F, Section F.4 removed reference to separate USARC MSC database server. Appendix H, Section H.3 updated help desk hours to reflect "1700" hours instead of "1800" hours.
R7C4	13 May 2011	Annual COOP update. Incorporates comments and findings from the annual COOP exercise and training conducted SEP 2010. Other changes made are to reflect virtualization of both the USARC Peachtree and the Prime Integrator facility at 6565 Arlington Blvd locations.
R7C5	1 July 2011	Updates are to incorporate comments received from the Government in relation to document version R7C4.
R7C6	30 September 2011	Updates are to incorporate new USARC backup methodology and new flow diagrams.

Rev.	Date	Description of Change
R7C7	17 November 2011	Updates are to incorporate comments received from the government in relation to document version R7C6.
R7C8	31 May 2012	Updates are to incorporate comments and annual COOP exercise after-action findings delivered to government 12 Dec 2011.

Approvals

Approval.....(b) (6) Title ..... Author Signature //s// ..... Date…05/23/2012
Product Approval ..... Title ..... AITS Quality Assurance Manager Signature.. (b) (6) ....Date… xx/xx/xxxx
Product Approval .....(b) (6) Title ..... AITS Enterprise Customer Relationships Manager Signature…//s// ....Date… xx/xx/xxxx
Product Approval …… (b) (6) Title …… Systems Operations Manager Signature …..//s//……Date…xx/xx/xxxx
Delivery Approval.....(b) (6) Title .....AITS Deliverables Management Lead Signature...../s/(b) (6) ..... Date…xx/xx/xxxx

Distribution

(b) (6) ..... RCAS Project Director (1 digital copy)
(b) (6) ..... ARNG-IMS Division Chief (1 digital copy)
(b) (6) ..... COR (1 digital copy)
(b) (6) ..... Chief BMO (1 digital copy)
(b) (6) ..... PD RCAS CM Manager (1 digital copy)
(b) (6) ..... PD RCAS Coordinator (1 digital copy)
(b) (6) ..... ARNG-IMS Enterprise Configuration Manager (1 digital copy)
(b) (6) ..... SAIC AITS Program Manager (1 digital copy)
(b) (6) ..... SAIC AITS Deputy Program Mgr/Business Mgr (1 digital copy)
(b) (6) ..... SAIC AITS Quality Assurance Manager (1 digital copy)
(b) (6) r ..... SAIC AITS Enterprise Operations Manager (1 digital copy)
(b) (6) ..... SAIC AITS Contracts Manager (1 digital copy)
(b) (6) ..... (1 digital copy)

Table of Contents

1 INTRODUCTION 1
1.1 Purpose 1
1.2 Scope 1
2 ASSUMPTIONS 2
3 ROLES AND RESPONSIBILITIES 3
4 RISKS 7
5 TYPE OF EMERGENCIES REQUIRING COOP PLAN ACTIVATION 8
5.1 System Priorities 9
5.2 Overall RCAS Priorities 9
5.3 External Interface Priorities 10
6 COOP NOTIFICATION AND COMMUNICATIONS PROCESS 12
6.1 COOP Notification 12
6.2 Personnel Accountability 14
6.3 Daily Status Reports 14
7 LEADERSHIP 15
7.1 Order of Succession 15
7.2 Delegation of Authority 15
8 BACKUP AND RECOVERY OPERATIONS 16
8.1 Backup Operations – RCAS USARC Production Environment 16
8.2 Backup Types – RCAS USARC Production Environment 17
8.2.1 Oracle Data Guard – Online Standby RCAS Replication 17
8.2.2 Veeam Backup and Recovery – VM Backups 17
8.2.3 RCAS Data Backups – External Off-Site Disk 17
8.3 Recovery Operations – RCAS USARC Production Environment 18
9 INFORMATION EXCHANGE REDIRECTION 19
10 ALTERNATE LOCATION OPERATIONS 19
10.1 PI Sustaining Engineer and Service Desk Personnel 19
10.2 USARC Operational Servers Fort Bragg 20
11 TRAINING AND TEST METHODS 21
11.1 Training 21
11.2 Test Methods and Exercises 21
11.2.1 Annually 21
11.2.2 Semi-Annually 22
11.2.3 Quarterly 22
11.2.4 Periodically 22
12 PLANS AND PROCEDURES 23
13 COOP DOCUMENT MAINTENANCE 25
13.1 Annually 25
13.2 Semi-Annually 25
APPENDIX A – COOP NOTIFICATION RECIPIENTS A–1
APPENDIX B – COOP STATUS COMMUNICATION B–2
COOP STATUS COMMUNICATION TEMPLATE B–2
APPENDIX C – DAILY STATUS NOTIFICATION C–3
APPENDIX D – COOP ACTIVATION PROCESS - 1 ..... D–5
APPENDIX E – COOP REPORTING - 2 ..... E–1

APPENDIX F – USARC ALTERNATE SITE PREPARATION - 3 ..... F–1
APPENDIX G – COOP ALTERNATE SITE PROMOTION – 4 ..... G–1
APPENDIX H – FALLS CHURCH SE/SD AND FT. BRAGG SD ALTERNATE SITE PROMOTION – 5 ..... H–1
APPENDIX I – COOP DEACTIVATION - 6 ..... I–1
APPENDIX J – USARC RETURN TO NORMAL – 7 ..... J–1
APPENDIX K – FALLS CHURCH SE/SD AND FT. BRAGG SD ALTERNATE SITE DEMOTION – 8 ..... K–1
APPENDIX L – USARC INFORMATION EXCHANGES L–1
APPENDIX M – SUCCESSION AND POINTS OF CONTACT M–1
APPENDIX N – USARC FORT BRAGG PRODUCTION SERVERS N–1
APPENDIX O – FALLS CHURCH SERVICE DESK O–1
APPENDIX P – USARC FORT BRAGG HELP DESK P–1
APPENDIX Q – SUSTAINING ENGINEERS Q–1
APPENDIX R – EMERGENCY CONTACT TEMPLATE – WALLET SIZE R–1
APPENDIX S – SAMPLE ANNUAL COOP TEST CHECKLIST S–2
APPENDIX T – ACRONYMS AND ABBREVIATIONS T–1

List of Figures

Figure 1. Backup Architecture RCAS USARC Production Environment 16
Figure 2. RCAS USARC Server Rack Diagram N–3

List of Tables

Table 1. MEF Priority 1
Table 2. System Outage Matrix 8
Table 3. Essential Function Priority 9
Table 4. USARC External Interfaces 10
Table 5. PI Order of Succession 15
Table 6. Veeam Snapshot Processing Schedule 17
Table 7. Alternate Work Locations 19
Table 8. Plans and Procedures 23
Table 9. USARC Information Exchanges L–1
Table 10. Enterprise Services Order of Succession M–1
Table 11. Falls Church, VA Succession Points of Contact M–2
Table 12. Fort Bragg Enterprise Services Points of Contact M–3
Table 13. PI Essential Personnel M–4
Table 14. PD RCAS Points of Contact M–6
Table 15. Vendor Points of Contact M–8
Table 16. Rack Configuration (Bottom to Top) N–4

1 INTRODUCTION

This Continuity of Operations Plan (COOP) implements the Reserve Component Automation Systems (RCAS) emergency operations, outlines policy and guidance. It establishes processes and procedures to ensure that essential functions and activities can be accomplished under a range of emergency conditions lasting no more than 30 days. In the event a condition requires longer than 30 days to resolve, the Prime Integrator (PI) will provide recommendations to Project Directorate (PD) RCAS to resolve the situation.

1.1 Purpose

The purpose of this plan is to:

- Ensure continuous operation of essential functions during service interruptions.
- Minimize disruption to essential functions performed at alternate locations.
- Provide communication and guidance to all staff members during COOP operations.
- Achieve a timely and orderly recovery from an emergency and resumption of normal operations.
- Ensure smooth succession of key PI personnel involved with essential functions.
- Maintain communications with internal and external contacts.
- Ensure procedures are in place to restore/recover services for the vital servers at the United States Army Reserve Command (USARC) (USARC RCAS Level 1 database, Major Subordinate Command (MSC) Level 2 database, and Level 1 and MSC web servers) upon activation of COOP.

1.2 Scope

Mission Essential Functions (MEFs) that this document covers include:

- Operational Support for the RCAS USARC production servers, Fort Bragg, NC.
- Service Desk Operations at PI sites 6565 Arlington Blvd, Falls Church, VA and Fort Bragg, NC.
- Sustaining Engineer (SE) Support, Falls Church, VA.

Table 1. MEF Priority

Priority	MEF
1	USARC Servers
2	Advanced Information Technology Systems (AITS) Service Desk
3	SEs

2 ASSUMPTIONS

- Disruption of operations may occur at any time, with or without warning.
- Events leading to relocation are localized to the 6565 Arlington Blvd., Falls Church, VA, and the Fort Bragg, NC, locations and/or their surrounding areas.
- Equipment currently in normal office spaces may be inaccessible.
- Primary means of system recovery will utilize a continually replicated, geographically-distributed warm site (Oracle Data Guard). A tertiary backup solution is comprised of physical Ethernet backup drives stored at the PI site at Aberdeen, NC.
- Communications and other external infrastructures will be sufficiently intact to allow implementation of this COOP.
- Army Knowledge Online (AKO) and other online repositories remain available for retrieval of plans, procedures, and Standard Operating Procedures (SOPs).
- Appropriate resources and funding will be available to support critical operations during the event.
- "Return to Normal" status refers to operations being restored as they were prior to activation of COOP. If a "Return to Normal" status cannot be achieved in under the 30 day window, the PI will recommend for approval to PD RCAS options that would allow for restoration of services.
- Minor interruptions to operations, such as the unavailability of the network system for two hours, will be handled utilizing procedures identified in applicable desk side procedures established by functional managers.
- Equipment hardware failures that are covered by equipment warranties will require two days to repair. Catastrophic hardware failures that require the procurement of new equipment will require at least 45 days.
- While COOP is activated, systems hosted at COOP facility will be kept at most current RCAS software release within the established 10 day Service Level Agreement (SLA) requirement. Systems at affected site will also be brought to most current RCAS baseline prior to COOP being deactivated.
- The targeted alternate COOP site will be stocked with appropriate equipment, furniture, utilities, and personnel and will have applicable levels of access in order for COOP to proceed.

3 ROLES AND RESPONSIBILITIES

The RCAS Project Director (PD) or their designee will:

- Activate COOP
- Assign a PD RCAS COOP Manager
- Notify PD RCAS COOP Manager of decision to activate COOP
- Approve COOP
- Deactivate COOP

The PI Program Manager (PM) or their designee will:

- Provide recommendations to the RCAS PD to activate COOP
- Activate COOP in the event that RCAS PD unavailable
- Assign a PI COOP Manager
- Approve the COOP
- Consult with the key PI personnel for input on COOP activation
- Notify the RCAS PD of the status of COOP Operations
- Provide recommendations to the RCAS PD to stand down COOP and return to normal operations

The PI COOP Manager will:

- Maintain and update COOP
- Activate COOP in the event that PI Program Manager or RCAS PD unavailable
- Publish and distribute updates to orders of succession as they occur
- Act as primary information/notification point of contact at PI 6565 Falls Church location during COOP events
- Notify necessary PI personnel of the decision to implement COOP via telephone and e-mail regardless of activation day/time
- Lead COOP training and exercises to ensure staff understand and can effectively implement the plan
- Create annual training, exercise schedule, exercise scenarios, and collect lessons learned
- Meet with necessary PI personnel and assess requirements that may impact the return to normal operations
- Collect information for and submit an after-action report within 14 business days after the AITS Program has returned to normal operations
- Include after-action items in the next COOP delivery cycle
- Maintain exercise training records and document and follow-up on problems uncovered during exercise or real-world events

- Document newly discovered risks detected during test or real-world events at the Joint Risk Management Control Board (JRMCB) for resolution
- Document PI personnel acknowledgment of changes in their responsibilities during COOP activation when changes have been made to COOP

The PD RCAS COOP Manager will:

- Notify PD RCAS Managers and the Program Executive Office, Enterprise Information Systems (PEO EIS) of the decision to implement COOP Plan
- Activate COOP in the event that RCAS PD unavailable
- Notify PI COOP Manager of decision to activate COOP
- Coordinate communications between PI personnel and PD RCAS personnel during COOP activation
- Participate in COOP training and exercises to ensure staff understands and can effectively implement the plan
- Provide input in the maintenance and updates to the COOP

The PI Enterprise Customer Relationship Manager (ECRM) will:

- Notify PI SE Manager that COOP has been implemented
- Notify PI Help Desk Manager that COOP has been implemented
- Provide daily status reports to PI Program Manager
- Notify PI SE Manager that COOP has been stood down
- Notify PI Help Desk Manager that COOP has been stood down

The PI Systems Operations Manager will:

- Notify PI USARC RCAS Services Manager that COOP has been implemented
- Activate COOP in the event that PI Program Manager unavailable
- Provide daily status reports to PI Program Manager
- Notify PI USARC RCAS Services Manager that COOP has been stood down
- Create Consent to Purchase (CTP) as necessary

The PI Service Desk/SE Manager will:

- Provide daily status reports to PI Program Manager
- Activate COOP in the event that PI Program Manager or PI COOP Manager unavailable
- Notify PI SE team that COOP has been implemented
- Perform the role of the PI ECRM in the event that person is unavailable
- Notify PI ECRM that PI SE team has reported to alternate sites and sites are operational
- Provide daily status reports to PI ECRM

- Notify PI SE team that COOP has been stood down
- Notify PI ECRM that PI SE team has reported to normal work locations and alternate sites are stood down
- Provide ECRM necessary information to create CTPs as necessary
- Notify PI Service Desk team that COOP has been implemented
- Notify PI ECRM that PI Service Desk team has reported to alternate sites and sites are operational
- Notify PI Service Desk team that COOP has been stood down
- Notify PI ECRM that PI Service Desk team has reported to normal work locations and alternate sites are stood down
- Provide ECRM necessary information to create CTPs as necessary

The PI USARC RCAS Services Lead will:

- Notify PI Systems Operations Manager of issues
- Act as primary information/notification point of contact at USARC site during COOP events
- Perform the role of the PI Systems Operations Manager in the event that person is unavailable
- Provide PI Systems Operations Manager with recommendations on best course of action to resolve issue
- Provide status reports to PI Systems Operations Manager
- Identify and recommend to PI Systems Operations Manager necessary information to complete CTP requests
- Ship backup Ethernet drives to Falls Church, VA as necessary
- Notify site personnel of COOP activation
- Notify site personnel of COOP deactivation

System Engineer Falls Church, VA will:

- Send status reports to PI SE Manager
- Prepare COOP environment to be promoted to primary site
- Load Ethernet drive data shipped from Fort Bragg site as necessary
- Make necessary Domain Name Service (DNS) change requests
- Configure necessary Information Exchange (IE) to point to promoted site
- Perform role of PI SE Manager in the event that person is unavailable
- Install and configure servers and operating systems as required

- Ensure all servers are Information Assurance Vulnerability Alert (IAVA) and Security Technical Implementation Guide (STIG) compliant
- Install/update all Operating System (O/S) patches and RCAS releases as required
- Ensure all servers have current anti-virus software In Accordance With (IAW) regulatory requirements
- Perform necessary server troubleshooting
- Monitor system logs, security logs, and application logs
- Perform detailed monitoring and tuning
- Perform security checklists on operating systems and system backups for each server
- Perform daily server operations including creating, deleting, and unlocking user accounts
- Troubleshoot Oracle issues as needed

System Administrator Fort Bragg, NC will:

- Prepare Fort Bragg site for demotion as necessary
- Prepare Fort Bragg site for promotion as COOP stood down
- Make necessary DNS change requests
- Configure necessary IE to point to Fort Bragg site
- Notify ENOSC of RCAS availability/unavailability as necessary
- Create weekly Ethernet backups as identified in Section 7
- Test environment prior to promotion of site
- Provide status reports to PI USARC RCAS Services Manager
- Perform role of PI USARC RCAS Services Manager in the event that person is unavailable

Database Administrator Fort Bragg, NC will:

- Backup and restore the database
- Contact Oracle Corporation for technical support
- Ensure that all necessary database files/logs are restored and operational prior to site promotion
- Ensure Oracle Data Guard is operational post-site promotion
- Provide status reports as necessary to PI Fort Bragg Site Manager

4 RISKS

A risk to the COOP Plan is the unavailability of the targeted COOP facility (6565 Arlington Blvd., Falls Church, VA). If such a condition occurs prior to the USARC COOP (Site Z) facility being in place (December 2011) then the USARC RCAS systems remain unavailable until such time the systems are restored to normal operations. The current USARC COOP facility, at Peachtree City GA, is being moved to Site Z at the end of calendar 2011 at which time the RCAS servers should be hosted at this facility as a tertiary COOP site.

5 TYPE OF EMERGENCIES REQUIRING COOP PLAN ACTIVATION

A COOP activation flowchart is contained in Appendices A through F of this document. Activation results when the RCAS USARC Site at Fort Bragg, NC and the PI Service Desks at Falls Church, VA are inoperable for extended periods of time, as determined be personnel onsite or by the RCAS PD (or their designate). Table 2 can be used as a guide for assisting site personnel or the RCAS PD in determining when to activate the COOP plan.

Table 2. System Outage Matrix

Severity	Anticipated Duration of System Outage	Examples
Condition I	Up to 12 hours	Power outage, minor troubleshooting
Condition II	12 to 24 hours	Extended service call required, minor flood or fire
Condition III	Greater than 24 hours and no more than 30 Days	Major system/hardware failure, catastrophic natural/manmade disaster
Condition IV	Greater than 30 Days	PI will provide recommendations to PD RCAS to resolve the situation.

Condition I events will normally not require COOP plan activation but could require activation if the minor event becomes part of a major event or ongoing operations could be substantially impacted. Site personnel or the RCAS PD may, at their discretion, activate the COOP plan for Condition I and II events. All Condition III events will require COOP plan activation, which include, but are not limited to the following:

- Major damage to hardware or communication systems
- Damage to files preventing operations, caused by either unintentional or malicious actions
- Conditions requiring relocation or abandonment of a major facility due to a disaster or emergency
- Malicious actions targeting the RCAS systems or data contained therein, with the intention to access, modify, or delete this data
- Conditions such as a natural disaster, complete power failure, or Heating, Ventilation, or Air Conditioning (HVAC) failure that damage or destroy an RCAS facility

In the event that a Condition III or Condition IV event is not resolved within the 30 days specified, the PI PM will provide recommendations to PD RCAS to resolve the situation.

5.1 System Priorities

In support of RCAS contingency operations, there are two sets of priorities:

- Overall RCAS System Priorities – First set of contingency priorities includes the actions necessary to reconstitute the hardware, software, and communications components that comprise RCAS (Section 5.2)
- External Interface (EI) Priorities – Second set of contingency priorities includes the actions necessary to reestablish communications with other external servers that send or receive data from the RCAS systems (Section 5.3)

5.2 Overall RCAS Priorities

The first priority during a contingency situation is to restore the operational availability and integrity of the RCAS systems to generate the data that is needed to support mission essential customers and services. These priorities include:

- Priority 1 – Validate Network Connectivity: The most critical action is to ensure network connectivity to the targeted COOP servers (6565 Arlington Blvd.) and external interfaces (USARC). This is necessary to be able to push Soldier data from any external interfaces to the USARC RCAS Database Server.
- Priority 2 – Restore Operations for the RCAS USARC Servers: These servers are the primary operational servers and are the interface points for external systems to access RCAS data.
- Priority 3 – Ensure Communications with the AITS Enterprise Service Desk (Falls Church, VA): As the primary program interface to the National Guard user community, the Enterprise Service Desk is the central clearinghouse for all National Guard inquiries.
- Priority 4 – Ensure Communications with the USARC RCAS Help Desk (Fort Bragg, NC): As the primary program interface to the United States Army Reserve (USAR) user community, the USARC Help Desk is the central clearinghouse for all Reserve inquiries.
- Priority 5 – Restore Operations for the Falls Church, VA SEs: Engineers are primary onsite support and Tier 3 phone support for the ARNG Soldiers supporting operational servers at ARNG sites.

Table 3. Essential Function Priority

Location	Priority	Function
Targeted COOP Facility	1	Validate Network Connectivity
Targeted COOP Facility	2	Restore Operations for the USARC RCAS Servers
Falls Church, VA	3	Ensure Communications with the AITS Enterprise Service Desk
Fort Bragg, NC	4	Ensure Communications with the USARC RCAS Help Desk

Location	Priority	Function
Falls Church, VA	5	Restore Operations for the Falls Church, VA Sustaining Engineers

5.3 External Interface Priorities

The USARC external interfaces identified in Table 4 will be restored. More detailed interface information can be found in Appendix L. Restoration priorities include:

- Priority 1 – Restore External Data Inputs: Once service is restored to mission essential services and customer, priority will be given to restoring communications with external systems providing data input to the RCAS servers, such as the Regional Level Application System (RLAS) which provides RCAS with Personnel, Resource Management, Training, and Mobilization data.
- Priority 2 – Restore Interfaces to Mission Essential Interfaces: Interfaces with mission essential customers will be restored as soon as possible, with a goal of 100% of these interfaces being operational within 24 hours of the activation of the contingency plan. These interfaces include communications with the Deployment and Reconstitution Tracking System (DARTS) which provides deployment data from RCAS to mobilization sites.

Table 4. USARC External Interfaces

IE Name	Level Used
Active Guard Reserve Management Information System (AGRMIS)	USARC
Army Stationing and Installation Plan (ASIP)	USARC
Checklist Management Automated System (CMAS)	MSC
DARTS	MSC
Digital Training Management System (DTMS) current Memorandum of Agreement (MOA)	USARC
Defense Joint Military Pay System (DJMS)	USARC
Federal Logistics Record (FEDLOG)	MSC
Field Accident Tablet System (FATS)	MSC
Force Management Support Agency (FMSA) current MOA	MSC
Global Command and Control System-Army (GCCS-A)	USARC
Integrated Data Reporting (IDR)	USARC

IE Name	Level Used
Logistics Integrated Database (LIDB)	USARC
Medical Operational Data System (MODS)	USARC
Program Optimization and Budget Evaluation (PROBE) current MOA	USARC
Property Book Unit Supply-Enhanced (PBUS-E)	MSC
Requirements Documentation System (RDS)	USARC
RLAS current MOA	MSC
Structure and Manpower Allocation System (SAMAS)	USARC
The Army Authorization Documents System (TAADS) 1,2, and 3	USARC
United States Army Forces Command-Aviation Resource Management System (FOMSCOM-ARMS)	MSC

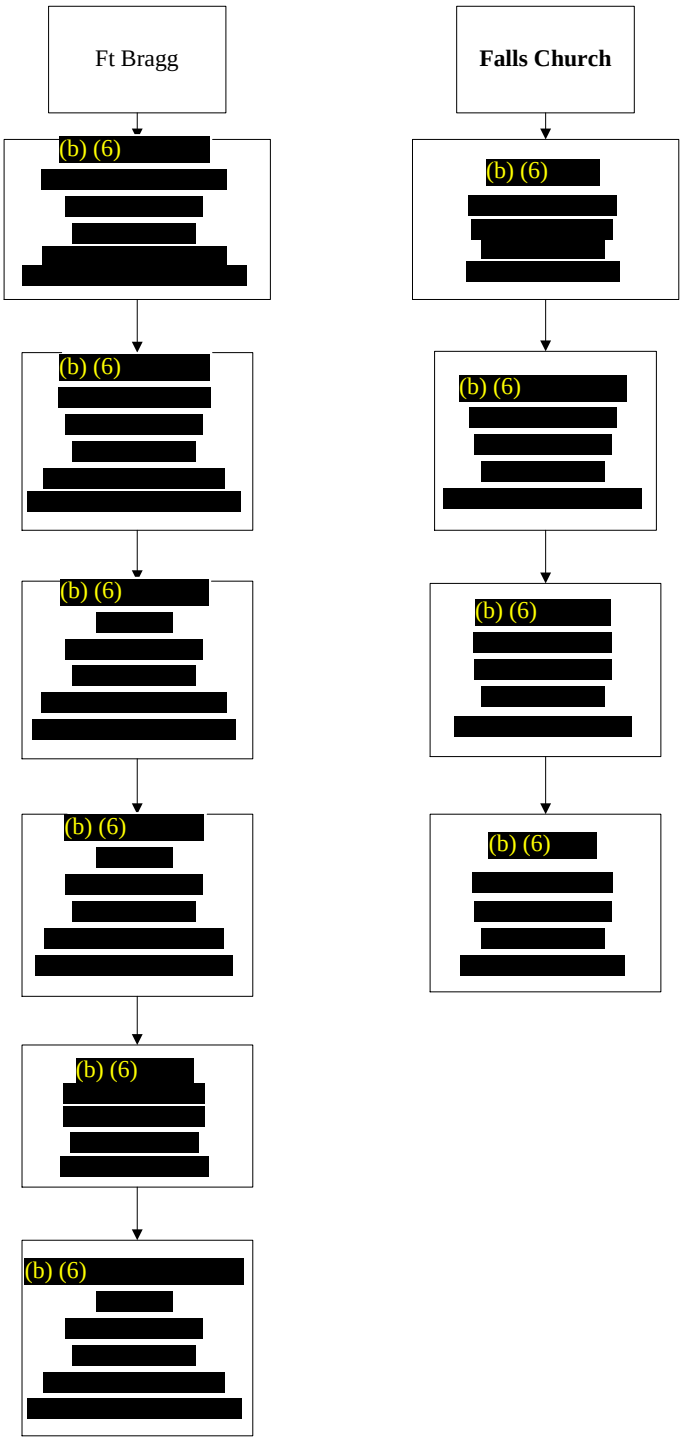
6 COOP NOTIFICATION AND COMMUNICATIONS PROCESS

This section provides an overview and guidance for personnel in regards to notification and communication processes to be utilized in the event of an unscheduled outage that requires COOP activation. Primary means of communication and notification will be handled utilizing phone, email, or text depending on the nature of the event and services available. Initial notifications and communications will be handled using all three methods until it can be determined what services are available at which time those will become the primary means of communication between sites/personnel. Applicable team leads will act as primary sources of information gathering and will be primary personnel responsible for providing status reports or other applicable communications.

6.1 COOP Notification

In the event that either a planned outage in anticipation of natural events (such as a hurricane) or an unplanned event causes an interruption in normal services that require COOP activation notifications will be sent to all personnel identified in Appendix A. Depending on site affected responding personnel will attempt to contact immediate supervisor or next applicable manager if supervisor cannot be reached. Utilizing communication templates in Appendix B. site personnel will provide necessary information needed that will be utilized for further decision making. Personnel should utilize the following phone tree when sending notifications.

Post-Event Accountability Phone Tree



6.2 Personnel Accountability

After an event happens managers need to determine the extent of the situation and who is available to work on the issues. Once an incident happens, either man made or natural, personnel must be accounted for in a timely manner in order to assess the magnitude of the situation and proper response needed to return services to their normal state prior to the incident. Site personnel, regardless of site, should immediately attempt to contact their immediate supervisor via phone, email, and text. Supervisors with direct reports upon notification that an event has occurred will also attempt to immediately contact personnel via phone, email, and text to ensure personnel are accounted for and to assess situation for proper decision making. Managers should utilize the phone tree with contact information as noted below.

6.3 Daily Status Reports

During an event it is necessary to provide reports to managers and supervisors in order to aid in decision making. To ensure that proper information needed is reported consistently, accurately, and in a timely manner site personnel must utilize the reporting templates provided in Appendix C.

7 LEADERSHIP

7.1 Order of Succession

Following a determination to activate the COOP, order of succession plans will be implemented. If the primary individual cannot be notified or located during an emergency situation, the next successor in line assumes responsibility. Methods of contacting individuals include telephone and email, BlackBerry, or cell phone. The next available official in the line of succession shall immediately begin to perform notification and other duties considered essential to COOP implementation until the principal or other higher successor becomes available and assumes control.

All essential functions identified fall under either the PI's ECRM group (SEs and Service Desk) or the PI Systems Operations Manager (Fort Bragg). Both the PI's ECRM and Systems Operations Manager have pre-designated individuals to make policy determinations and decisions. These individuals are authorized to act on behalf of the ECRM and Systems Operations Manager. Order of Succession can be found in Appendix M. The order of succession for the identified MEFs is displayed in Table 5.

Table 5. PI Order of Succession

Fort Bragg, NC	Falls Church, VA
PI Systems Operations Manager	PI ECRM
PI USARC RCAS Services Lead	PI Enterprise Service Desk/SE Manager
PI Site System Administrator (SA)	PI SE Lead

7.2 Delegation of Authority

If either the PI ECRM or Systems Operations Managers cannot be immediately contacted upon COOP activation, or if confirmation is received that the official will not be capable of performing his or her duties, authority is automatically delegated to the succeeding individual. In most instances, full authority to make all decisions for that position has been granted. Authority for specific functions can be re-delegated, as necessary. Delegation of authority is terminated when the higher official assumes his or her responsibilities, or by formal direction from higher authority. Implementation of the COOP should not be delayed due to the unavailability of one or more senior officials.

8 BACKUP AND RECOVERY OPERATIONS

8.1 Backup Operations – RCAS USARC Production Environment

Primary backup and recovery for the RCAS USARC production environment consists of three separate approaches:

- A continually replicated geographically-distributed warm site
- Automatic Virtual Machine (VM) snapshots stored on a local secondary storage subsystem
- Routine weekly RCAS data backups copied to encrypted external hard drives and stored off-site

Each of these backup methods is intended to provide options in the event of a recovery incident. By designing the backup and recovery solution using multiple technologies, a wide range of possible risks are mitigated, including the possible failure of one of the backup systems (Figure 1).

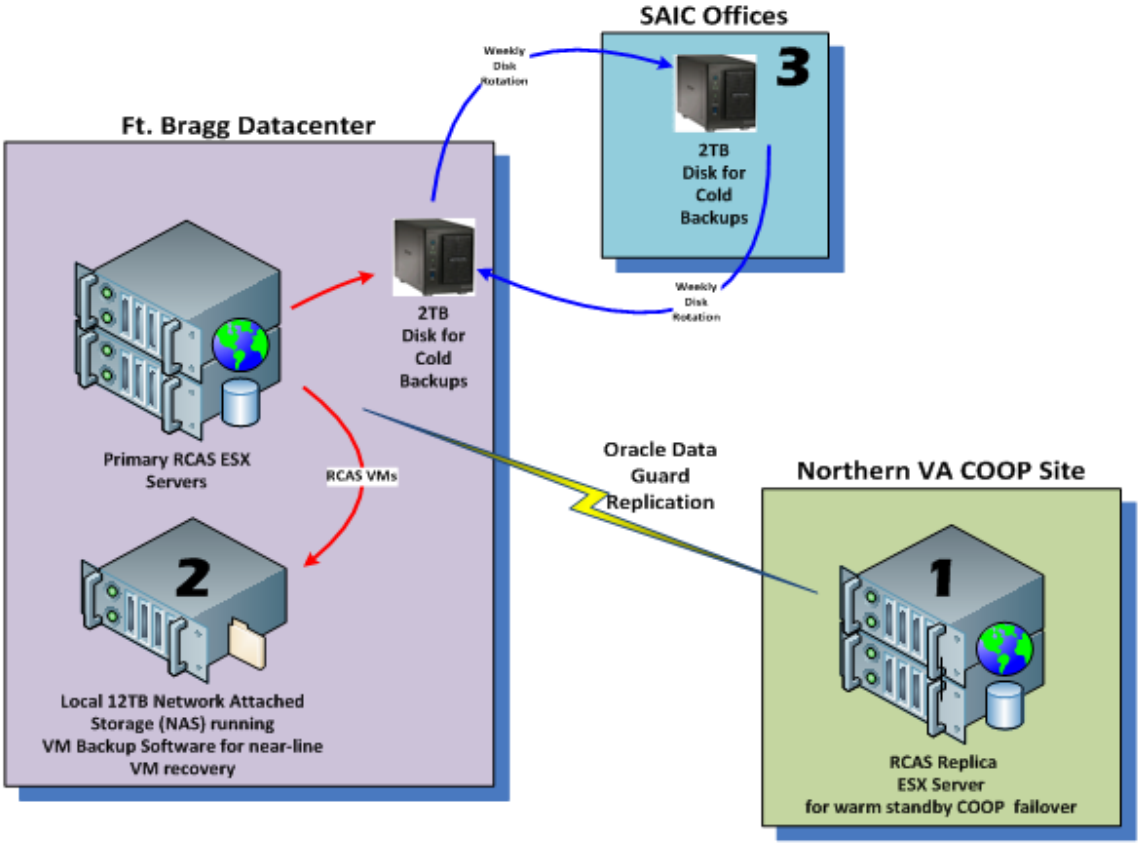


Figure 1. Backup Architecture RCAS USARC Production Environment

8.2 Backup Types – RCAS USARC Production Environment

8.2.1 Oracle Data Guard – Online Standby RCAS Replication

The Northern Virginia COOP Site in Figure 1 references the use of Oracle Data Guard to ensure high availability, data protection, and disaster recovery through a comprehensive set of services that create, maintain, manage, and monitor a standby replica database to enable production Oracle databases to survive disasters and data corruptions. Data Guard is a built-in part of the Oracle 10g/11g database software designed to continually send all changes from the primary RCAS database over to a secondary RCAS. If the production database becomes unavailable because of a planned or an unplanned outage, the system administrators can switch the replica database to the production role, minimizing the downtime associated with the outage. Data Guard will act as the primary backup solution that will provide near real-time duplication of data and transactions between the production servers located at Fort Bragg, NC and the targeted warm site at 6565 Arlington Blvd.

Data Guard backup schedule includes production systems connected with Data Guard continually replicate data to the replica server.

8.2.2 Veeam Backup and Recovery – VM Backups

The Fort Bragg Datacenter in Figure 1 references how RCAS currently operates entirely as virtualized servers with an array of VMware ESX hosts. Installed on a separate dedicated server with over 8 Terabyte (TB) of usable storage, Veeam Backup and Recovery software protects the RCAS environment by continually and automatically making image copies, or snapshots, of the running RCAS VMs. VM snapshots are full copies or smaller differential snapshots of just the changes since the last full copy was created. In the event that a production RCAS VM becomes corrupted or unavailable, the systems administrators can restore the latest VM snapshot of any of the RCAS servers.

The Veeam backup schedule includes a Veeam snapshot backup taken nightly of two RCAS Web servers and the RCAS database server to dedicated server storage separate from the production Storage Area Network (SAN).

Table 6. Veeam Snapshot Processing Schedule

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Type	Diff	Full	Diff	Diff	Full	Diff	Diff

8.2.3 RCAS Data Backups – External Off-Site Disk

The Science Applications International Corporation (SAIC) Offices in Figure 1 references the Ethernet backups created every Sunday night. The RCAS database is taken offline and the data is copied in a cold backup out to a directory on the primary SAN. After the backup is generated, it is also copied to an encrypted external drive. On Monday morning, the external hard drive connected to the RCAS server is swapped with a second hard drive and the first is taken back to an off-site SAIC facility and locked in a cabinet. Each week, this swapping of external hard drives rotates the off-site storage of the RCAS data. This is not a full system backup, but only a copy of the data that could be reloaded into an empty RCAS server. These offsite drive backups provide a means for recovery in the event of a catastrophic failure of the Oracle Data Guard solution.

8.3 Recovery Operations – RCAS USARC Production Environment

Recovery of RCAS USARC production servers depends upon the nature and expected duration of the recovery event. If available, the Veeam backups can be used if the primary production VMware hosts are still operational. In the event of the Fort Bragg full outage, the Data Guard connected replica servers at the targeted alternate facility (6565 Arlington Blvd., Falls Church, VA) will then become primary servers after appropriate DNS and IE interfaces are updated. In the event of a catastrophic failure, external disk backups will be shipped to an alternate facility and the database server will be restored utilizing the backup drives. Recovery operations would constitute the following:

- Restore from drive as applicable
- Promote Data Guard servers as primary
- DNS redirected to point to new servers
- IE updates/rerouting as needed
- IA scans/remediation completed
- Final Operating Capability achieved
- Notification to ENOSC that systems are available

9 INFORMATION EXCHANGE REDIRECTION

The requirements necessary for each IE to establish and maintain the exchange of information with RCAS are documented in an RCAS/USARC MOA, a Memorandum of Understanding (MOU), and/or a System Interface Agreement (SIA), signed by the United States Army Program Executive Office Enterprise Information Systems (USA PEO EIS), RCAS Project Director and the responsible agency representative for the system or application with which RCAS is exchanging data. In the event that COOP is activated the SEs would need to redirect applicable IEs, as found in Appendix L. SEs will ensure that IEs are redirected in accordance with instructions located in the latest applicable IE administration guides found on AKO and also identified in section 12, table 8.

10 ALTERNATE LOCATION OPERATIONS

Targeted alternate work locations and/or COOP sites as identified by the COOP involve locations at both PI employee primary residences and the PI facility at 6565 Arlington Blvd. In the event that service interruptions cause the activation of COOP, depending on site affected, PI personnel will move to these alternate locations until service is restored at primary locations. Alternate locations for both PI personnel at the PI facility in Falls Church, VA, and PI Help Desk personnel at the Fort Bragg, NC location will be personnel's primary residences. Targeted alternate location for restoring RCAS USARC operational capabilities will be the PI facility in Falls Church, VA.

The targeted alternate locations will be considered operational when the PI Program Manager has set up operations, has connectivity to RCAS servers, and can begin directing operations. Essential PI staff members, as identified in this plan, or as directed by the PI PM, will report for work at targeted alternate locations so that essential functions can begin within 12 hours of the time when the decision was made to implement the COOP. Upon arrival at targeted alternate locations, staff members will report to the PI ECRM or designee. If necessary, shifts will be set up to accommodate all personnel who need to work.

Table 7. Alternate Work Locations

PI Personnel/USARC Servers	Alternate Locations
Fort Bragg Personnel	Primary Residence
PI Sustaining Engineers	Primary Residence
PI Service Desk Personnel	Primary Residence
USARC Server Operations	PI Facility Falls Church, VA

10.1 PI Sustaining Engineer and Service Desk Personnel

PI Service Desk and SE personnel will use their residence as their primary COOP site. All personnel have laptops that are loaded with all software needed to perform duties remotely. Primary means of communications for personnel within these groups are email and phone. All SEs are assigned BlackBerry devices and laptops. SEs meeting all security requirements have VPN capabilities that allow for remote administration of servers at the PI facility in Falls Church, VA. Service Desk personnel in Falls Church, VA are also equipped with laptops that have remote capabilities to the NGB Remedy system. RCAS USARC Fort Bragg, NC, Help Desk

personnel are also equipped with a laptop that allows remote capabilities to the USARC Unicenter system.

10.2 USARC Operational Servers Fort Bragg

In the event that the operational servers at USARC Fort Bragg, NC become unavailable, the targeted alternate COOP site is the PI facility at 6565 Arlington Blvd. Falls Church, VA. PI SEs will initiate the activation and standing up of the servers at Falls Church, VA, and become primary administrators until the Fort Bragg, NC location can be restored. Personnel from Fort Bragg, NC will stay in place to reconstitute the site. In the event that personnel at the Fort Bragg, NC site are unable to perform required duties, SEs will deploy to Fort Bragg, NC site to support reconstitution efforts and will remain until COOP is stood down or personnel become available.

PI facility at Falls Church, VA will house a set of servers as a warm site for COOP of Fort Bragg, NC. Oracle Data Guard will be the primary source of data backup and restoration while Ethernet drive backups will be secondary. Server clones and database cold backups will be created at the Fort Bragg, NC location and Ethernet drives created will be stored at a PI facility (140 Aqua Shed Ct., Aberdeen, NC 28315). These drives will be shipped and loaded at the Falls Church, VA location if a catastrophic event happens that will not allow for the Data Guard solution to activate. Current RCAS web server images will be maintained at 6565 Arlington Blvd. facility and will be staged and ready for deployment.

11 TRAINING AND TEST METHODS

Training, tests, and exercises to familiarize staff members with the process and their roles during an emergency ensure that systems and equipment are maintained in a constant state of readiness, and validate various aspects of the COOP. Managers may use snow days, power outages, server crashes, and other ad-hoc opportunities to assess preparedness of the staff. PI Managers will ensure that their employees are familiar with the RCAS COOP. The PI COOP Manager will conduct a comprehensive debriefing after each exercise for the participants to identify systemic weaknesses in plans and procedures and recommend COOP revisions.

11.1 Training

Training for personnel with contingency plan responsibilities will complement testing. Training will be provided annually; new hires who will have plan responsibilities will receive training as part of the RCAS program orientation. New hires that will have COOP responsibilities will be identified on the RCAS on-boarding checklist which will notify the PI COOP Manager that the new hire will require an overview of the COOP during orientation. Further training will occur prior to a person assuming operational duties, and refresher training will be conducted at least annually.

Training may be conducted as a combination of training classes, brown bag sessions, and mini-exercises that will be conducted independent from the Annual COOP testing. Personnel with COOP responsibilities will be trained to the extent that they are able to execute their respective recovery procedures without aid of the actual COOP document. This is an important goal in the event that paper or electronic versions of the plan are unavailable for the first few hours resulting from the extent of the disaster. Personnel who have COOP responsibilities are cross trained in their respective areas in the event that personnel with primary responsibilities are unavailable, e.g. all SEs know how to maintain the servers, create/restore backups in the event the SE Lead is unavailable. Personnel will be trained on the following plan elements:

- Chain of command
- Purpose of the plan
- Cross-team coordination and communication
- Reporting procedures
- Security requirements
- Team-specific processes (Notification/Activation, Recovery, and Reconstitution Phases)
- Individual responsibilities (Notification/Activation, Recovery, and Reconstitution Phases)

11.2 Test Methods and Exercises

The RCAS Program will follow the Tests, Training and Exercises Schedule as outlined below.

11.2.1 Annually

- Provide designated successors with annual refresher briefings
- Provide annual COOP awareness briefings or orientation to the entire workforce
- Key personnel review and refresh roles and responsibilities

- Reevaluate targeted alternate operating facility for suitability and functionality
- Provide staff training on the maintenance of server backups
- Conduct an annual Table Top or Live exercise focusing on a specific problem related to COOP implementation that, at a minimum, contains:
  - Opportunity for COOP personnel to demonstrate their familiarity with the COOP and the capability to continue essential functions
  - The movement of COOP personnel to targeted alternate work locations.
  - Communications/Notifications capabilities
  - After-Action report to include any lessons-learned (all exercise participants will submit information)
- Addresses system recovery on alternate platforms from backup media
- Coordination among recovery teams
- Ability to maintain or recover internal and external connectivity
- Maintain appropriate system performance using alternative equipment IAW approved SLAs
- Restoration of normal operations

11.2.2 Semi-Annually

Plans are tested for the recovery of critical information systems, services, and data.

11.2.3 Quarterly

- Test internal and external communications capabilities, or more frequently, as directed
- Test the alert, notification, and activation procedures

11.2.4 Periodically

- Brief designated successors, when named, on their responsibilities
- Provide an orientation to newly appointed COOP personnel
- Update orders of succession, as necessary, and distribute revised orders as they occur

The PI COOP Manager will maintain training records identifying the date of the exercise, personnel involved, the scope of the exercise, and lessons learned. Any problems encountered will be assigned a PI Point of Contact (POC) who will recommend a solution to PD RCAS. Once a solution is identified, it will be exercised to ensure its effectiveness and viability.

12 PLANS AND PROCEDURES

Applicable plans and procedures used by personnel involved with the identified essential functions are provided in Table 8.

Table 8. Plans and Procedures

Plan/Procedure	Location
RCAS Database Administration Guide	https://www.us.army.mil/suite/doc/23282532
RCAS Web Application Server Guide	https://www.us.army.mil/suite/doc/23861527
Current RCAS release documentation	https://www.us.army.mil/suite/files/7428250
IE Administration Guide – Level 1	https://www.us.army.mil/suite/doc/29607028
IE Administration Guide – Level 2	https://www.us.army.mil/suite/doc/29607027
USARC Systems Administration SOP	https://collaboration.saic.com/sites/AITS/AITS%20Portal%20Documents%20New/Forms/AllItems.aspx?RootFolder=%2fsites%2fAITS%2fAITS%20Portal%20Documents%20New%2fAITS%20Procedures%2fFS%20Series%20%28Field%20Support%20and%20Sustainment%29&FolderCTID=&View=%7bDD91CFEE%2dE8A2%2d4DB4%2d9CAC%2d480EE5D737F5%7d
Service Desk SOP	https://collaboration.saic.com/sites/AITS/PreAward%20Proposal%20Documents/Forms/AllItems.aspx?RootFolder=%2fsites%2fAITS%2fPreAward%20Proposal%20Documents%2fRCAS%2fEnterprise%20Services%2fService%20Desk%2fSOP&FolderCTID=0x01200098CDD6459A7A154AAC0CC53722C5B4AD&View=%7b9C9EE9FE%2d7BE5%2d46B7%2d9901%2d50EA17FD60C9%7d
SE SOP	https://collaboration.saic.com/sites/AITS/PreAward%20Proposal%20Documents/Forms/AllItems.aspx?RootFolder=%2fsites%2fAITS%2fPreAward%20Proposal%20Documents%2fRCAS%2fEnterprise%20Services%2fSustaining%20Engineering%2fSOP&FolderCTID=0x01200098CDD6459A7A154AAC0CC53722C5B4AD&View=%7b9C9EE9FE%2d7BE5%2d46B7%2d9901%2d50EA17FD60C9%7d
Service Desk Personnel Desk Side Procedures	6565 Arlington Blvd. Falls Church, VA – Cubicle 4-063
Sustaining Engineer Desk Side Procedures	6565 Arlington Blvd. Falls Church, VA – Room 347 top drawer of file cabinet
Service Desk Personnel Desk Side	Combined Headquarters, USARC

Procedures	4710 Knox Street, Fort Bragg, NC Cubicle 2-
System Administrator Desk Side Procedures	Combined Headquarters, USARC 4710 Knox Street, Fort Bragg, NC Cubicle 2-

13 COOP DOCUMENT MAINTENANCE

The PI COOP Manager will be responsible for initiating COOP documentation updating actions annually. Notices will be sent to all necessary PI Managers as a reminder to update individual plans in both the COOP document and those in Section 12 based on the schedule outlined below. Those documents in Section 10 are the USARC Systems Administration SOP, Service Desk Personnel Desk Side Procedures, and the Sustaining Engineer Desk Side Procedures. The PI COOP Manager will gather and resolve conflicts in all inputs and update the RCAS COOP plan. Key personnel will meet at least annually to discuss and provide input to the RCAS COOP plan. This organization will be known as the COOP Working Group (CWG). Any additional Federal or local guidelines published since the last COOP update will be incorporated.

PI Managers will report any changes to their individual COOP to the COOP Manager as soon as possible after the change occurs, but no later than 30 calendar days. In addition, information obtained from after action reports submitted following testing and exercises will be incorporated into the RCAS COOP.

13.1 Annually

The COOP document will be reviewed and updated for content and completeness or as deemed necessary by significant changes in configuration or environment.

13.2 Semi-Annually

The COOP Manager will verify and update if necessary:

- Order of Succession
- Delegation of Authority
- Changes in Personnel
- Update Phone Lists
- Update Office Room Numbers

APPENDIX A – COOP NOTIFICATION RECIPIENTS

The COOP Notification Recipients list Table 9 is intended to identify USARC, PD RCAS and PI personnel of the COOP activation and deactivation.

Table 9. COOP Notification Recipients

POC	Email
[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

POC	Email
(b) (6)	(b) (6)
(b) (6)	(b) (6)
(b) (6)	(b) (6)
(b) (6)	(b) (6)
(b) (6)	(b) (6)
(b) (6)	(b) (6)
(b) (6)	(b) (6)
(b) (6)	(b) (6)
(b) (6)	(b) (6)
(b) (6)	(b) (6)
(b) (6)	(b) (6)
(b) (6)	(b) (6)
(b) (6)	(b) (6)
(b) (6)	(b) (6)
(b) (6)	(b) (6)
(b) (6)	(b) (6)
(b) (6)	(b) (6)

APPENDIX B – COOP STATUS COMMUNICATION

The COOP Status Communication template will be used to provide updates and information necessary for further decision making.

COOP STATUS COMMUNICATION TEMPLATE

Email Subject Line:

COOP //Date of COOP DDMMMYYYY// RCAS Production Environment

COOP Activation has been required for the RCAS Suite (Production Environment).

Current status as of HHMM (Time of message creation):

(Add brief Summary of the latest status)

Remedy Ticket:HD nnnnn

Outage Start Date: DDMMMYYYY

Estimated Time to Restore (ETR):
Unknown or Update of estimated duration (minutes, hours, days, weeks etc.)

Action:

Briefly summarize actions moving toward resolution.

List equipment below:

- **Web Server:** ZNC121C2308RL41
- **Web Server:** ZNC121C25MN3451
- **Database Server:** ZNC12145XBJYB1

APPENDIX C – DAILY STATUS NOTIFICATION

Applicable site personnel will utilize a standard notification format in order to ensure that consistent information is provided regardless of personnel sending. Status updates will be provided twice a day (early morning and prior to close of business) or as situations dictate.

RCAS Daily Status

Section 1 – Situation Awareness

Fill in pertinent information such as status of (Use Go/No Go, e.g. Power – No Go):

Power

Water

Cooling Systems

Building Access

Server Room Access

Communications (Phone/Email)

Network

Section 2 – RCAS Server Status

Server Rack

Power Backup

Physical Servers

Storage Devices

Remote Access

Console Access

Section 3 – RCAS Application Status

Information Exchanges

RCAS Database for Level 1

RCAS Database for Level 2

RCAS Web Server Level 1

RCAS Web Server Level 2

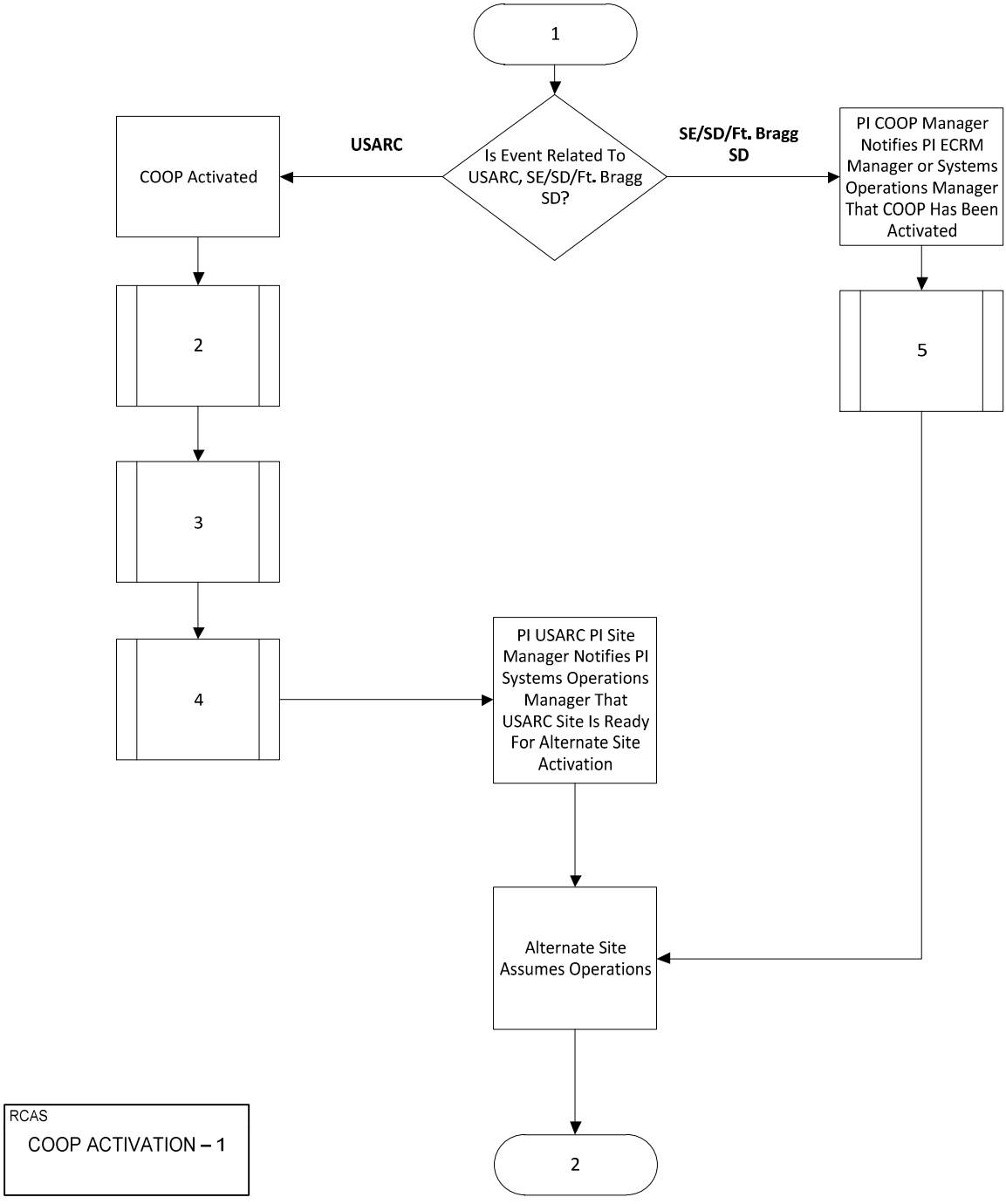
RCAS Level 1 Applications

RCAS Level 2 Applications

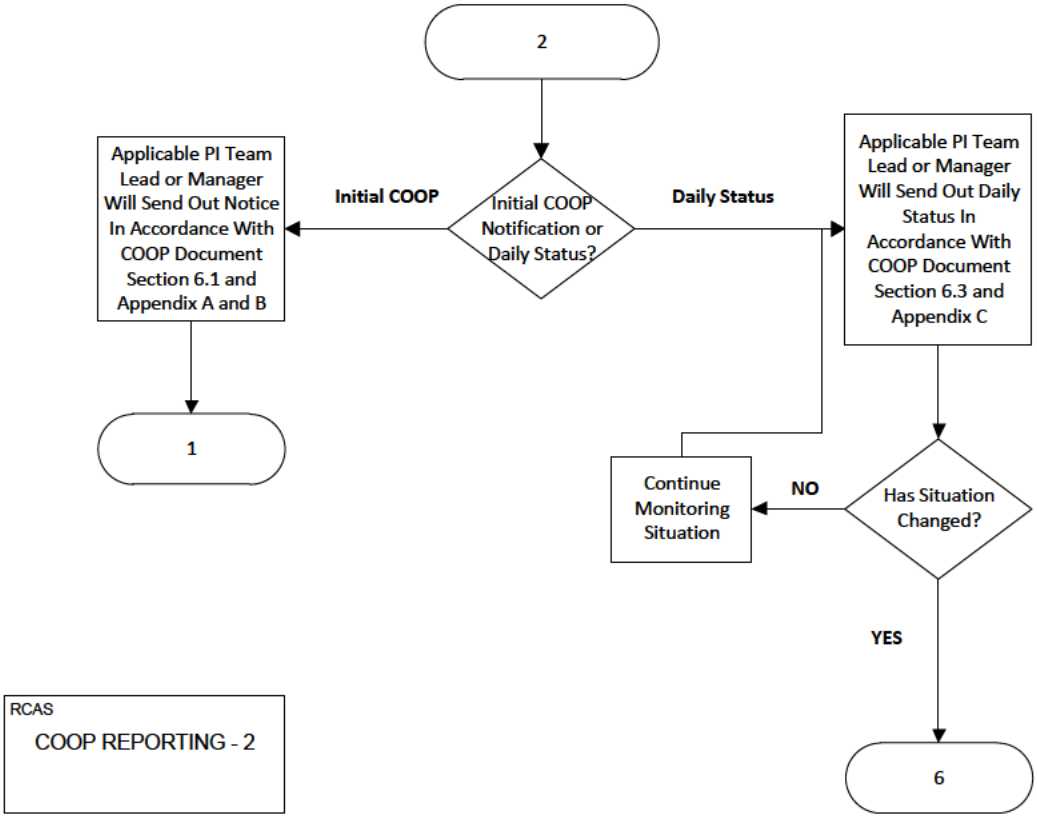
Section 3 – Misc. Notes (please include additional information in bulleted form)

APPENDIX D – COOP ACTIVATION PROCESS - 1

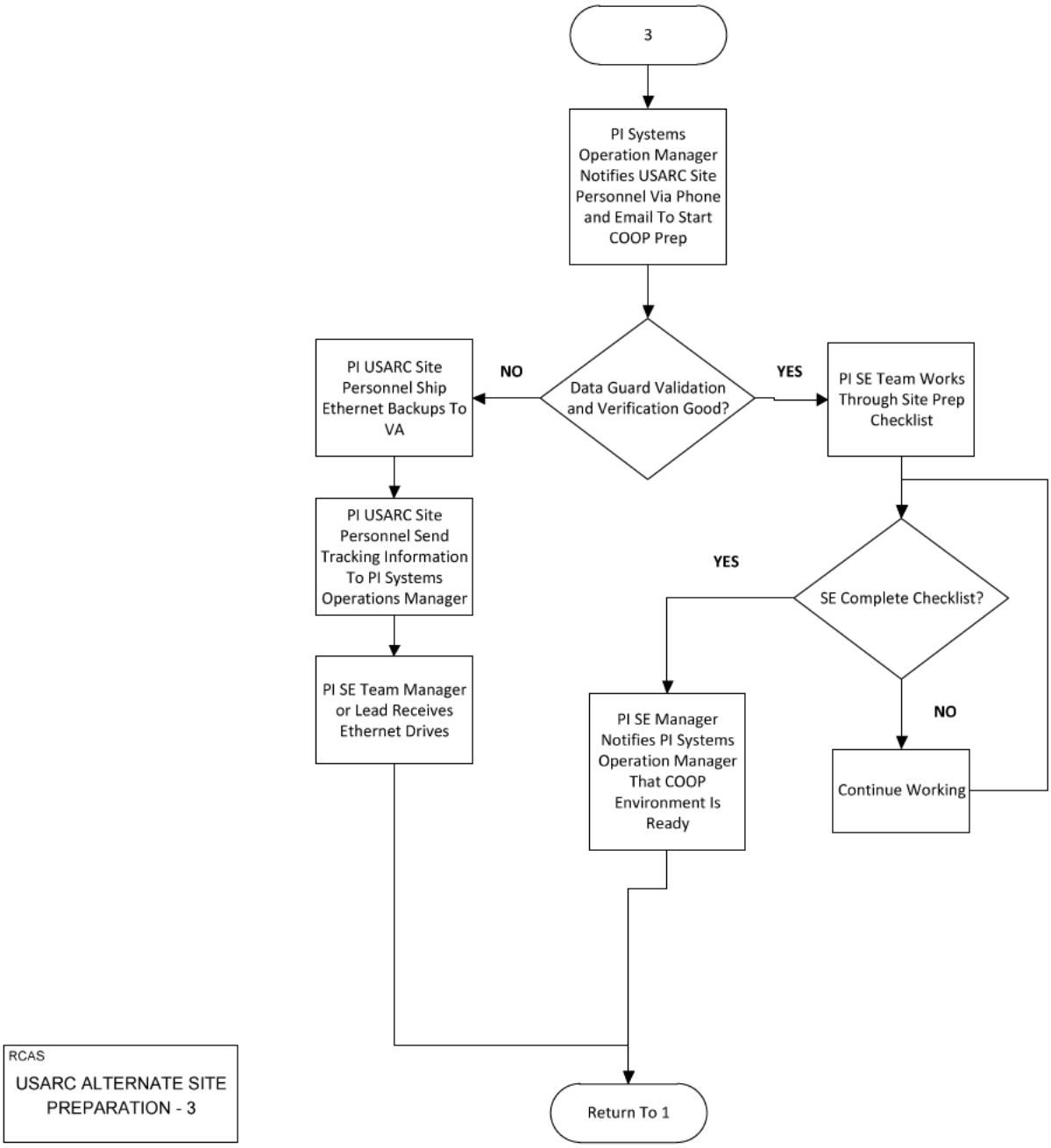
Appendices D through K comprise the COOP processes from activation through deactivation. For ease of use and expediency processes have been referred to by numeric form on all flow charts. Appendix titles include wording as to let users understand what each process is.



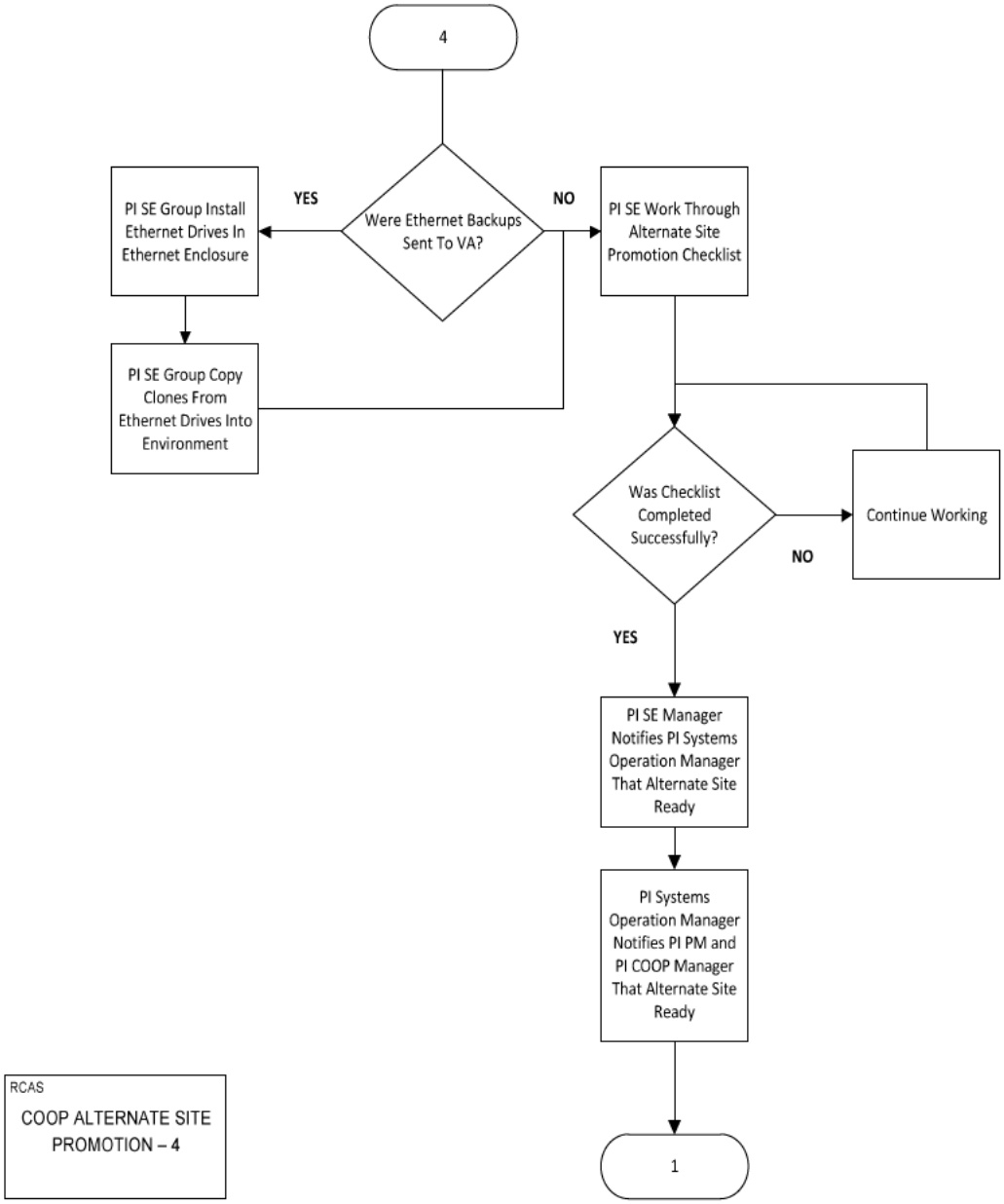
APPENDIX E – COOP REPORTING - 2



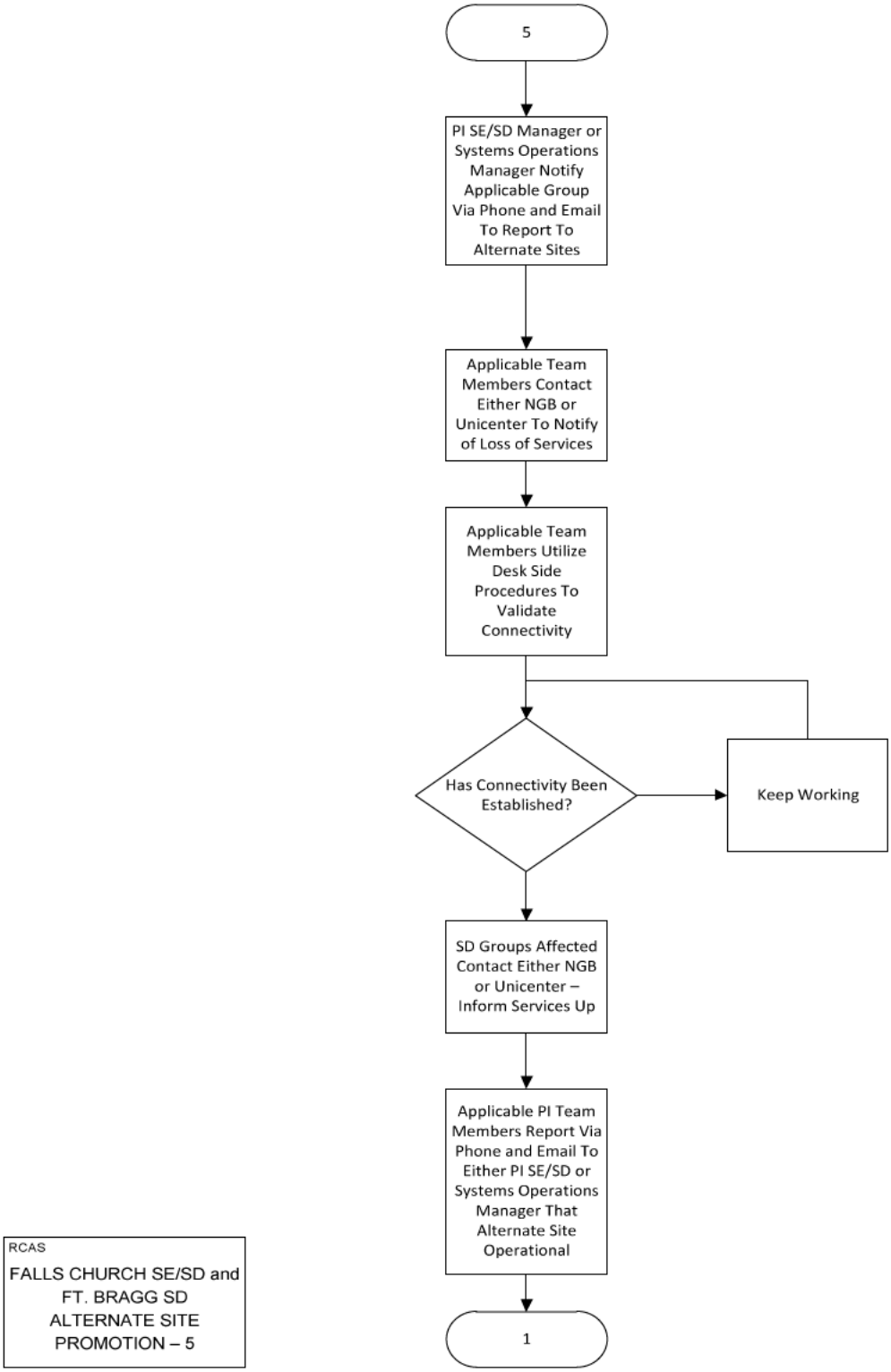
APPENDIX F – USARC ALTERNATE SITE PREPARATION - 3



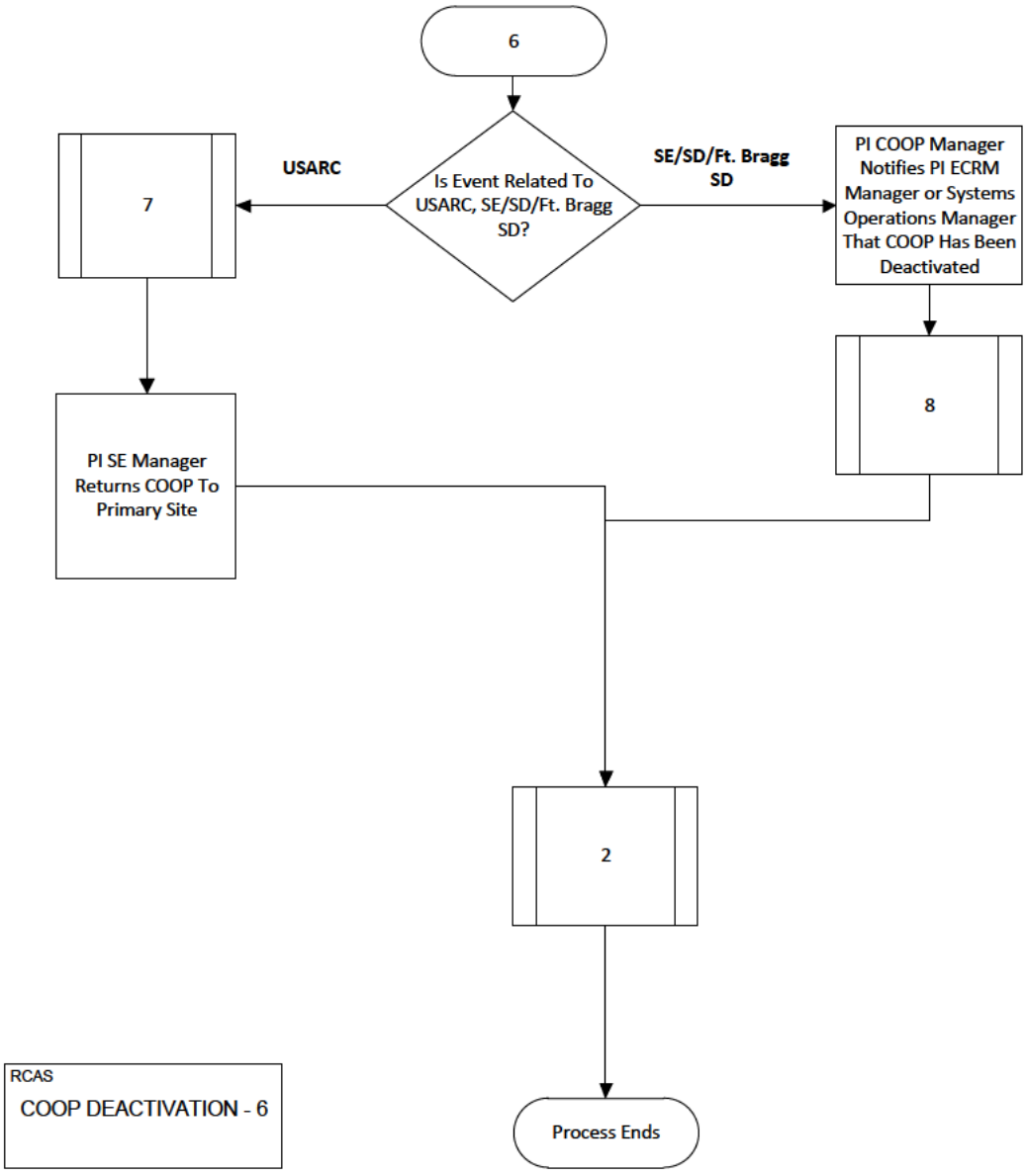
APPENDIX G – COOP ALTERNATE SITE PROMOTION – 4



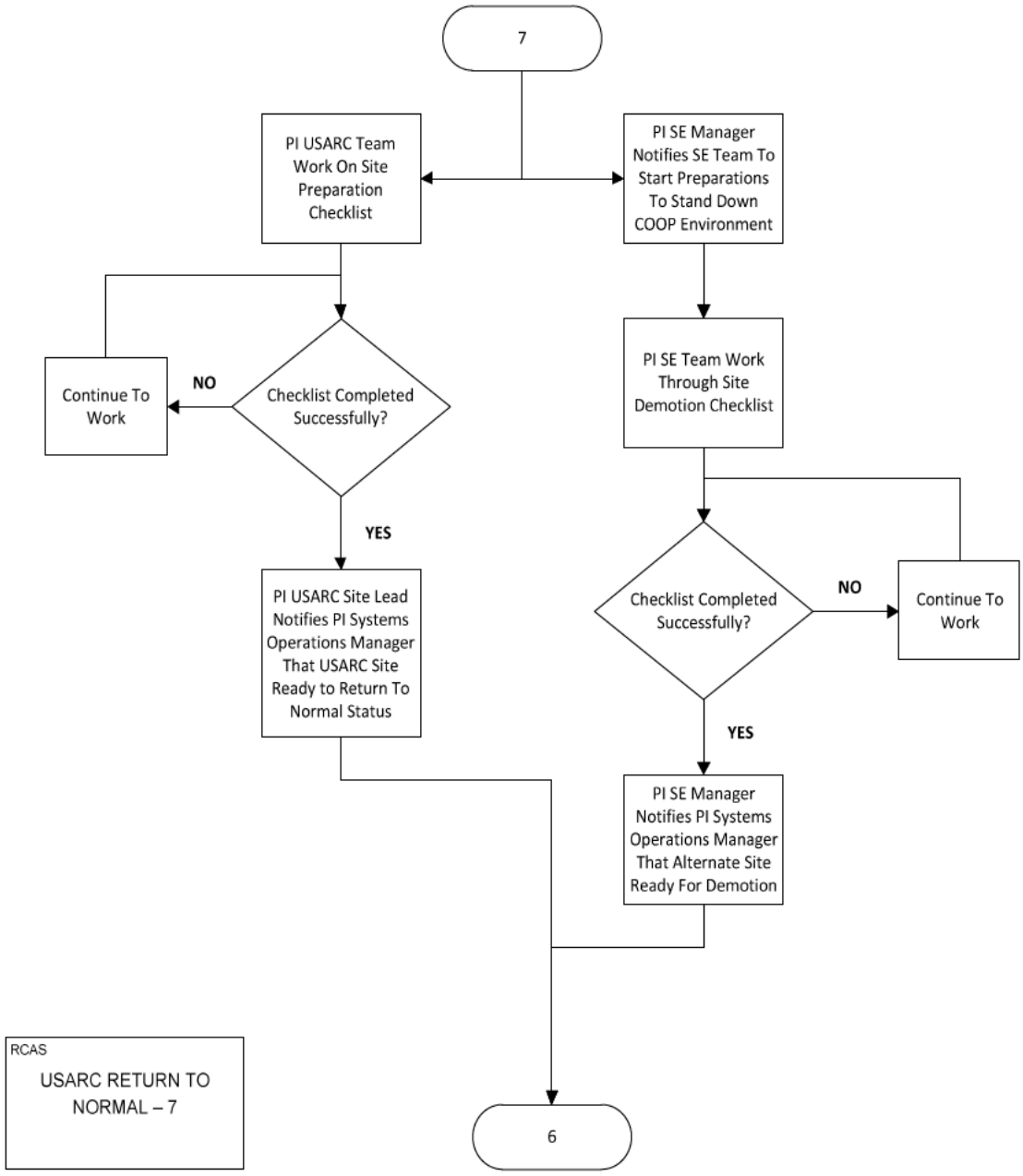
APPENDIX H – FALLS CHURCH SE/SD AND FT. BRAGG SD ALTERNATE SITE PROMOTION – 5



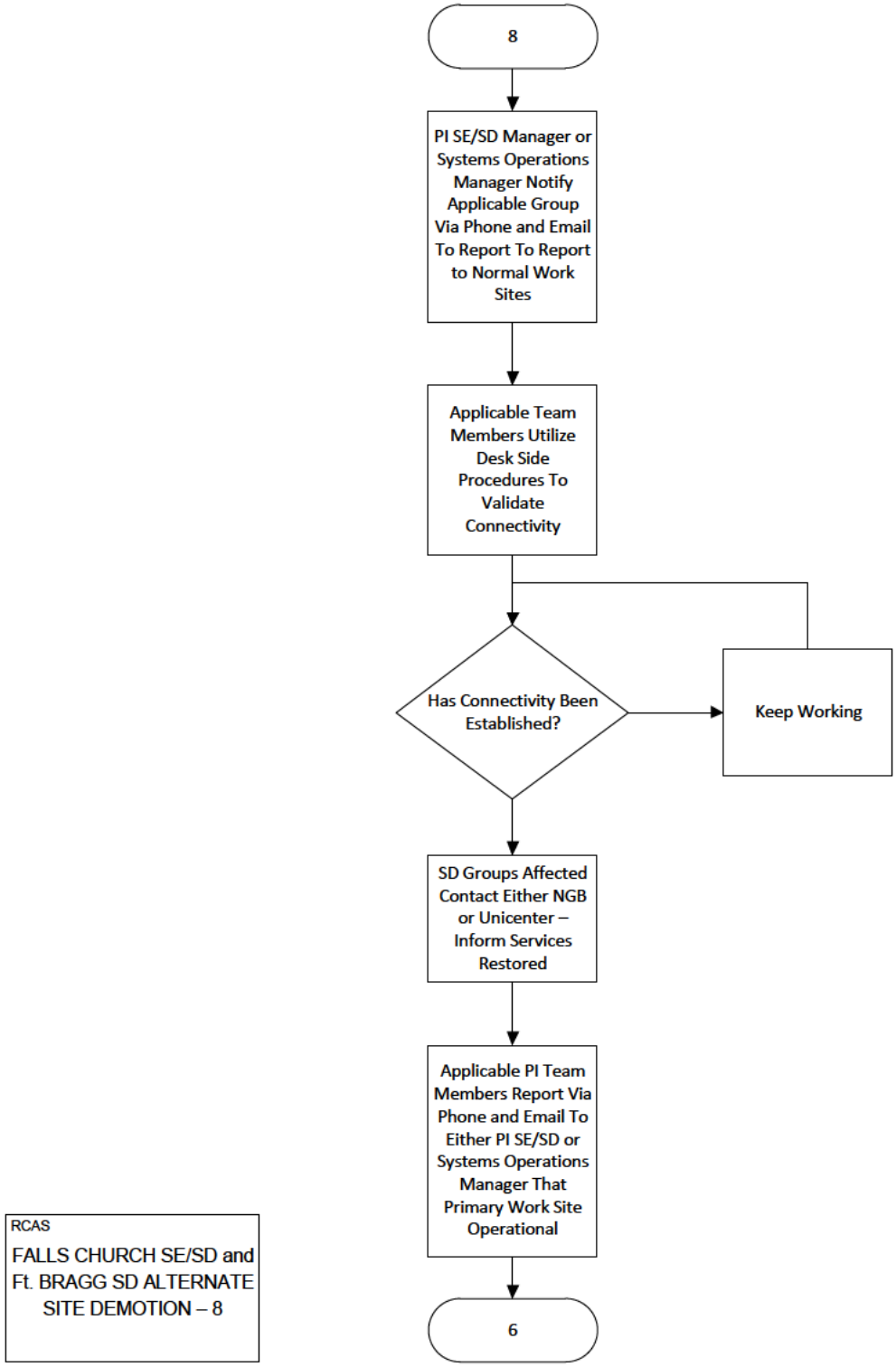
APPENDIX I – COOP DEACTIVATION - 6



APPENDIX J – USARC RETURN TO NORMAL – 7



APPENDIX K – FALLS CHURCH SE/SD AND FT. BRAGG SD ALTERNATE SITE DEMOTION – 8



APPENDIX L – USARC INFORMATION EXCHANGES

The requirements necessary for each IE to establish and maintain the exchange of information with RCAS are documented in an RCAS/USARC MOA, a Memorandum of Understanding (MOU), and/or a System Interface Agreement (SIA), signed by the United States Army Program Executive Office Enterprise Information Systems (USA PEO EIS), RCAS Project Director and the responsible agency representative for the system or application with which RCAS is exchanging data.

The Port/Internet Protocol (IP) for the USARC IEs are not applicable (N/A) with the exception of the following:

- DJMS – 21/Yes
- LIDB – 1,521/Yes
- MODS – 22/Yes
- TAADS 1,2,3 – 1,521/Yes
- DARTS – Yes/Yes

Table 9. USARC Information Exchanges

System/App Name	Source	Location	How Received/Sent	Frequency	Applications
Active Guard Reserve Management Information System (AGRMIS)	USARC (ARMY)	Level 1 USARC	RCAS Full Time Support (FTS) application user generates an American Standard Code for Information Interchange (ASCII), pipe delimited, data file that may be written on Compact Disc (CD)/Digital Video Disc (DVD), e-mailed, or otherwise and sends to the Human Resources Command (HRC) (supporting the United States Army Reserve (USAR)	Outbound As Needed	FTS

System/App Name	Source	Location	How Received/Sent	Frequency	Applications
Army Force Generation (ARFORGEN) Army Reserve Expeditionary Force (AREF)	USARC (ARMY)	USARC	USARC ARFORGEN user creates an Excel file and sends to RCAS Level 1-USARC via CD/DVD/e-mail. RCAS SA places file on the RCAS WEB Application Server where it is loaded into the RCAS IDB by an MPDV application User	Inbound As Needed	MPDV
Army Stationing and Installation Plan (ASIP)	Headquarters Department of the Army (HQDA)-Assistant Chief of Staff for Installation Management (ACSIM) (ARMY)	USARC	A database file on CD/DVD received at Level 1-USARC, RCAS DBA loads an ASCII, semicolon delimited, data file to directory on RCAS Web Application server; RCAS IE Loader application loads data to RCAS database, data is replicated to RCAS Level 2-MSC applications.	Inbound Semi-Annually	Safety and Occupational Health (SOH) Force Management (FM)
Army Safety Management Information System (ASMIS) – under development	Continental United States (CONUS) Replacement Center (CRC) (ARMY)	USARC	Outbound Level 2-MSC SOH App User, moves data to RCAS Web Server, App pushes data to Level 1-USARC Database Server. Upon approval, Level 1-USARC User sends via Web services; pulls back reference files; Application moves files to IDB SOH tables. Inbound data replicated to Level 2-MSC.	Outbound/ Inbound As Needed	SOH

System/App Name	Source	Location	How Received/Sent	Frequency	Applications
Command And Control Verifier System (C2VS)	USARC (ARMY)	Level 2-MSC	C2VS SA pushes organization data to USARC staging server. Oracle Data Integrator (ODI) tool pulls data to RCAS Level 1-USARC IDB and moves it to Level 2-MSC RCAS IDB.	Inbound Daily	CORE (Hierarchy) MPDV
Checklist Management Automated System (CMAS)	SOH (ARMY)	MSC	RCAS SOH-CMAS user uploads Field Inspection results to SOH from CMAS as Inspection Findings via Hypertext Transfer Protocol Secure (HTTPS) RCAS SOH-CMAS application user exports Inspections and Checklists from SOH to CMAS.	Inbound As Needed Outbound as needed	SOH CMAS
Component (COMPO)	HQDA- United States Army Force Management Support Agency (USAFMSA) (ARMY)	USARC	RCAS A&R application user logs on to USAFMSA-COMPO; copies zipped Oracle Dump files, unzip and create temp tables in RCAS database. RCAS IE Loader application loads data into RCAS database.	Inbound Annually	A&R
Deployment and Reconstitution Tracking Software (DARTS)	FORSCOM (ARMY)	Level 2-MSC	RCAS MPDV application user creates export files and sends data to DARTS' web service in Extensible Markup Language (XML) format from MPDV via HTTPS	Outbound As Needed	MPDV

System/App Name	Source	Location	How Received/Sent	Frequency	Applications
Defense Civilian Personnel Data System-USAR (DCPDS-USAR)	Civilian Personnel Operations Center (CPOC) (ARMY)	USARC	CPOC POC pushes ASCII, tab delimited, data files to USARC secure File Transfer Protocol (FTP) server, RCAS DBA moves data to RCAS web app server, data is loaded to Level 1-RCAS USARC IDB, and replicated to Level 2-MSC.	Inbound As Needed	SOH All Apps
Defense Joint Military Pay System (DJMS)	Defense Finance & Accounting Service (DFAS) (DoD)	LEVEL 1 USARC	DJMS POC stages a zipped, password protected, ASCII file on DJMS' Secure File Transfer Protocol (SFTP) server. Level 1-RCAS USARC DBA moves file into USARC Secure FTP server and to RCAS web app server. Level 1-USARC pushes data to Level 2-MSC IDBs.	Inbound Monthly	MPDV
Digital Training Management System (DTMS)	Training & Doctrine Command (TRADOC) (ARMY)	USARC	RCAS MPDV application user clicks on hyperlink provided on Graphical User Interface (GUI) enters user Identification (ID). Training data exchanged using web service via HTTPS between DTMS and Level 1-RCAS USARC IDB, and replicated to Level 2-MSC.	Inbound Daily As Required Outbound Daily As Required	MPDV

System/App Name	Source	Location	How Received/Sent	Frequency	Applications
Engineering and Base Operations Support System (ENBOSS)	HQDA- ACSIM (ARMY)	USARC	USARC DBA FTPs from ENBOSS server to USARC secure FTP server within network; RCAS DBA moves to RCAS IDB, data is replicated to Level 2-MSC RCAS IDB.	Inbound Monthly	A&R SOH
Field Accident Tablet System (FATS)	SOH (ARMY)	MSC	Accident investigations are conducted in the field and uploaded to SOH as new accidents via HTTPS. Reference data can be exported from SOH and loaded to FATS.	Inbound As Needed Outbound As Needed	SOH FATS
Federal Logistics Information System (FEDLOG)	United States Army Materiel Command (USAMC), Logistics Support Activity (LOGSA) (ARMY)	USARC	FEDLOG database files on DVDs received at USARC, RCAS DBA loads an ASCII, fixed length, data file to directory on web app server; RCAS IE Loader application loads data to RCAS database; data is replicated to Level 2-MSC applications.	Inbound As Needed	FM SOH MPDV
Force Management Support Agency (FMSA)	USARC (ARMY)	USARC	RCAS FTS application user creates an ASCII data file that may be written on CD/DVD, e-mailed, or otherwise and sends to USAFMSA via USARC FTS POC.	Outbound As Needed	FTS

System/App Name	Source	Location	How Received/Sent	Frequency	Applications
FORSCOM-Aviation Resource Management System (ARMS)	FORSCOM (ARMY)	MSC	FORSCOM team gives a comma delimited, text file on media to Safety Officer who manually uploads via HTTPS to SOH as Inspection Findings.	Inbound As Needed	SOH
Global Command and Control System-Army (GCCS-A)	HQDA (ARMY)	USARC	RCAS DBA retrieves five zipped ASCII, pipe delimited, data files from behind AKO; moves data to RCAS web app server, data loaded to Level 1-RCAS USARC IDB; and replicated to Level 2-MSC.	Inbound Bi-Weekly	FM All Apps
Integrated Data Reporting (IDR)	USARC (ARMY)	USARC	RCAS FTS application user generates an ASCII, tab delimited, data file that may be written on CD, e-mailed, or otherwise and sends to IDR.	Outbound As Needed	FTS
Logistics Integrated Data Base (LIDB) Logistics Information Warehouse (LIW)	USAMC, LOGSA (ARMY)	USARC	Oracle to Oracle DB link. Data replicated to Level 2-MSC.	Inbound As Needed	MPDV

System/App Name	Source	Location	How Received/Sent	Frequency	Applications
Medical Occupational Data System (MODS)	Surgeon General (ARMY)	USARC	MODS pushes zipped file to USARC FTP servers. RCAS DBA, with password, copies files to RCAS and unzips; software pkg moves file to IDB staging tables. Level 2-MSC schedules a link to get files from Level 1-USARC IDB.	Inbound Daily	MPDV
Property Book Unit Supply Enhanced (PBUSE)	HQDA (ARMY)	MSC	PBUSE application user logs on to PBUSE and creates ASCII text data file and moves file to RCAS manually (e.g., via CD, e-mail, or copied to a shared drive) where it is loaded into MPDV application via HTTPS.	Inbound As Needed	MPDV
Program Optimization and Budget Evaluation (PROBE)	USARC (ARMY)	USARC	RCAS FTS application user clicks on hyperlink provided on GUI, enters user ID and password for access to PROBE, and manually moves flat file to RCAS web app server for load into RCAS IDB.	Inbound As Needed	FTS
Requirements Documentation System (RDS)	HQDA-USAFMSA (ARMY)	USARC	E-mail received at Level 1-USARC, data replicated to Level 2-MSC as part of the RCAS application.	Inbound As Needed	A&R

System/App Name	Source	Location	How Received/Sent	Frequency	Applications
RLAS	USAR (ARMY)	MSC	RCAS DBA moves data files from RLAS to RCAS web app server; RCAS IE Loader application loads files into RCAS database.	Inbound As Needed	MPDV SOH
Structure and Manpower Allocation System (SAMAS)	HQDA- Office of the Deputy Chief of Staff, Operations & Plans (ODCSOPS) (ARMY)	USARC	Zipped file received via e-mail at National Guard Bureau (NGB) and USARC sites; data loaded in RCAS IDB and replicated to Level 2-MSC in the RCAS application.	Inbound Semi-Annually	FM
The Army Authorization Documents System (TAADS)	HQDA- USAFMSA (ARMY)	USARC	RCAS FM application user logs on with user ID and establishes link from RCAS IDB at NGB and USARC to USAFMSA, and copies files to RCAS IDB for use.	Inbound Daily, Monthly, Annually	FM

APPENDIX M – SUCCESSION AND POINTS OF CONTACT

PI personnel with primary responsibilities over the essential functions identified in the identified in Table 10, Table 11, and

. The SE and Service Desk essential functions fall within the PI's ECRM group whereas RCAS USARC operations fall under the PI Systems Operations Manager. In the event that the PI ECRM is unable to be reached, succession and delegation of authority for SE or Service Desk would fall to the PI Enterprise Service Desk/SE Manager and then the to the PI SE Lead.

In the event that the PI Systems Operations Manager is unable to be reached succession would fall to the PI USARC RCAS Services Manager if issues involve the Fort Bragg, NC site and then to the PI System Administrator. Table 13 and Table 14 provide pertinent contact information for key PI and PD RCAS personnel. Table 15 provides contact information for primary vendors and technical support.

Table 10. Enterprise Services Order of Succession

Position Title	Successor Title	Conditions	Program Responsibility
PI Enterprise Customer Relations Manager	PI Enterprise Service Desk/SE Manager for events involving SEs/Help Desk	If the PI Enterprise Services Manager or the PI Systems and Operations Manager cannot respond during an incident or emergency situation	Full
	PI SE Lead for events involving SEs and Service Desk		
PI Systems Operations Manager	PI USARC RCAS Team Lead for events at Fort Bragg, NC		
	PI System Administrator for events at Fort Bragg, NC		

Table 11. Falls Church, VA Succession Points of Contact

Position	Name	Contact Information
PI DTTP/Enterprise Services Manager	(b) (6)	(b) (6)
PI Enterprise Service Desk/SE Manager	(b) (6)	(b) (6)
PI SE Lead	(b) (6)	(b) (6)
PI Systems Operations Manager	(b) (6)	(b) (6)

Table 12. Fort Bragg Enterprise Services Points of Contact

Position	Name	Contact Information
PI RCAS Operations Team Lead	(b) (6)	(b) (6)
PI RCAS System Administrator	(b) (6)	(b) (6)
PI RCAS System Administrator	(b) (6)	(b) (6)
PI Help Desk Analyst	(b) (6)	(b) (6)
PI RCAS Database Administrator (DBA)	(b) (6)	(b) (6)

Table 13. PI Essential Personnel

Position	Name	Contact Information
PI Program Manager	(b) (6)	(b) (6)
PI Deputy Program Manager	(b) (6)	(b) (6)
PI Systems Operations Manager	(b) (6)	(b) (6)
PI DTTP/Enterprise Services Manager	(b) (6)	(b) (6)
PI Project Manager RCAS Product Families	(b) (6)	(b) (6)
PI COOP Manager	(b) (6)	(b) (6)
PI Information Assurance Manager	(b) (6)	(b) (6)

Position	Name	Contact Information
PI Infrastructure Asset Manager	(b) (6)	(b) (6)
PI AITS Procurement	(b) (6)	(b) (6)
PI Database Team Lead	(b) (6)	(b) (6)
PI Back Office Team Lead/Deputy Project Manager RCAS Product Families	(b) (6)	(b) (6)
PI SE Team Lead	(b) (6)	(b) (6)
PI Enterprise Service Desk Team Lead	(b) (6)	(b) (6)
PI Enterprise Service Desk Analyst	(b) (6)	(b) (6)

Position	Name	Contact Information
PI SE Team Member	(b) (6)	(b) (6)
PI SE Team Member	(b) (6)	(b) (6)
PI SE Team Member	(b) (6)	(b) (6)
PI Training Manager	(b) (6)	(b) (6)

Table 14. PD RCAS Points of Contact

Position	Name	Contact Information
RCAS PD	(b) (6)	(b) (6)
PD RCAS Deputy Director	(b) (6)	(b) (6)
PD RCAS Chief Engineering Officer	(b) (6)	(b) (6)

Position	Name	Contact Information
PD RCAS Information Assurance Manager	(b) (6)	(b) (6)
PD RCAS COOP Manager	(b) (6)	(b) (6)
PD RCAS Life Cycle Support Division Chief	(b) (6)	(b) (6)

Table 15. Vendor Points of Contact

Position	Name	Contact Information
Dell Computer Hardware, Enterprise Software and Solutions (CHESS) Inside Sales Representative	(b) (6)	(b) (6)
Dell CHESS Technical Sales Representative	(b) (6)	(b) (6)
CISCO and American Power Conversion Corp. (APC) CHESS World Wide Technology (WWT) Representative	(b) (6)	(b) (6)
Dell Warranty Number	N/A	Telephone number: 1-800-876-3355 Administrator will be prompted to enter hardware service tag number.
Oracle Technical Support	N/A	Database team will utilize the Support.Oracle.com website. Database team members have the applicable username and password.
Microsoft Technical Support	N/A	Back Office team will utilize the Microsoft 1-800-936-3100 telephone support number to submit trouble tickets. Back Office team members have the applicable account information.
Hewlett Packard Warranty Information	N/A	Telephone number: 800-334-5144 Administrator will be prompted to enter hardware service tag number.

APPENDIX N – USARC FORT BRAGG PRODUCTION SERVERS

N.1 Architecture

The architecture consists of the current RCAS baseline builds for both a RCAS USARC Level 1 and RCAS USARC MSC Level 2 consolidated database server. RCAS USARC Level 1 and RCAS USARC MSC Level 2 web servers are also in the environment.

N.2 Purpose

The RCAS USARC servers provide access to the RCAS applications which are used by USARC units to aid in mobilization activities. Currently, both the Level 1 and Level 2 servers are housed at the USARC Fort Bragg, NC, location. These servers provide the USARC with 24/7 access to live data that is used by units to perform day-to-day functions and aid in mobilization. In the event that these servers are unavailable, there is no current failover solution. Servers will either have to be troubleshot or rebuilt. Impact to field and mobilizing units could be substantial.

Note: Computer Associates (CA) Wily monitoring tools provide site personnel with automated notification of server availability issues associated with the servers which allow personnel to respond quickly regardless of time/day.

N.3 Virtualization

The current RCAS USARC server environment is virtualized and utilizes VMware High Availability (HA) capabilities. VMware HA utilizes the VMware Vmotion software that monitors the physical virtual host server and its operating system for failure. In the event of failure, the hosted virtual servers will migrate to the next designated host server with minimal service interruptions. The HA capability is not part of a COOP solution but is a feature that prevents short-term interruptions in service while the physical host server is serviced. Current architecture involves four (4) Dell R710 servers hosting three virtual server images as identified in section N.1. A staging area for creating image clones or preparing clones for deployment has also been established.

N.4 Data/Server Backups

Database cold backups and server clones are created during the regularly scheduled weekly outage windows and when the RCAS service baselines are upgraded. Cold backups are created during the weekly maintenance outage. Server clones are created during baseline upgrades. Backups and clones are created weekly and transferred to an Ethernet drive backup solution per Section 8 and validated in accordance with the local RCAS Administrator Operations Manual (SOP/Maintenance). The Operations Manual is located in the top cabinet of the Database Administrator’s (DBA’s) cubicle located at USARC HQ G-2/6 - Cubicle 2N2501-111 in Fort Bragg, NC and also online at the location provided in Section 12 .

N.5 Addresses

USARC Level 1/Level 2 Database	ZGA114A45XBJYB1.ar.ds.army.mil
USARC Level 1 Web	ZGA114114C2308RL41.ar.ds.army.mil
MSC Web	ZGA114C25MN3451.ar.ds.army.mil
Domain Controller	N/A third party control

N.6 Rack Configuration

Figure 2 displays the current rack configuration to include where virtualized server instances are hosted. Table 16 provides additional information in regards to specific rack locations of equipment and equipment type.

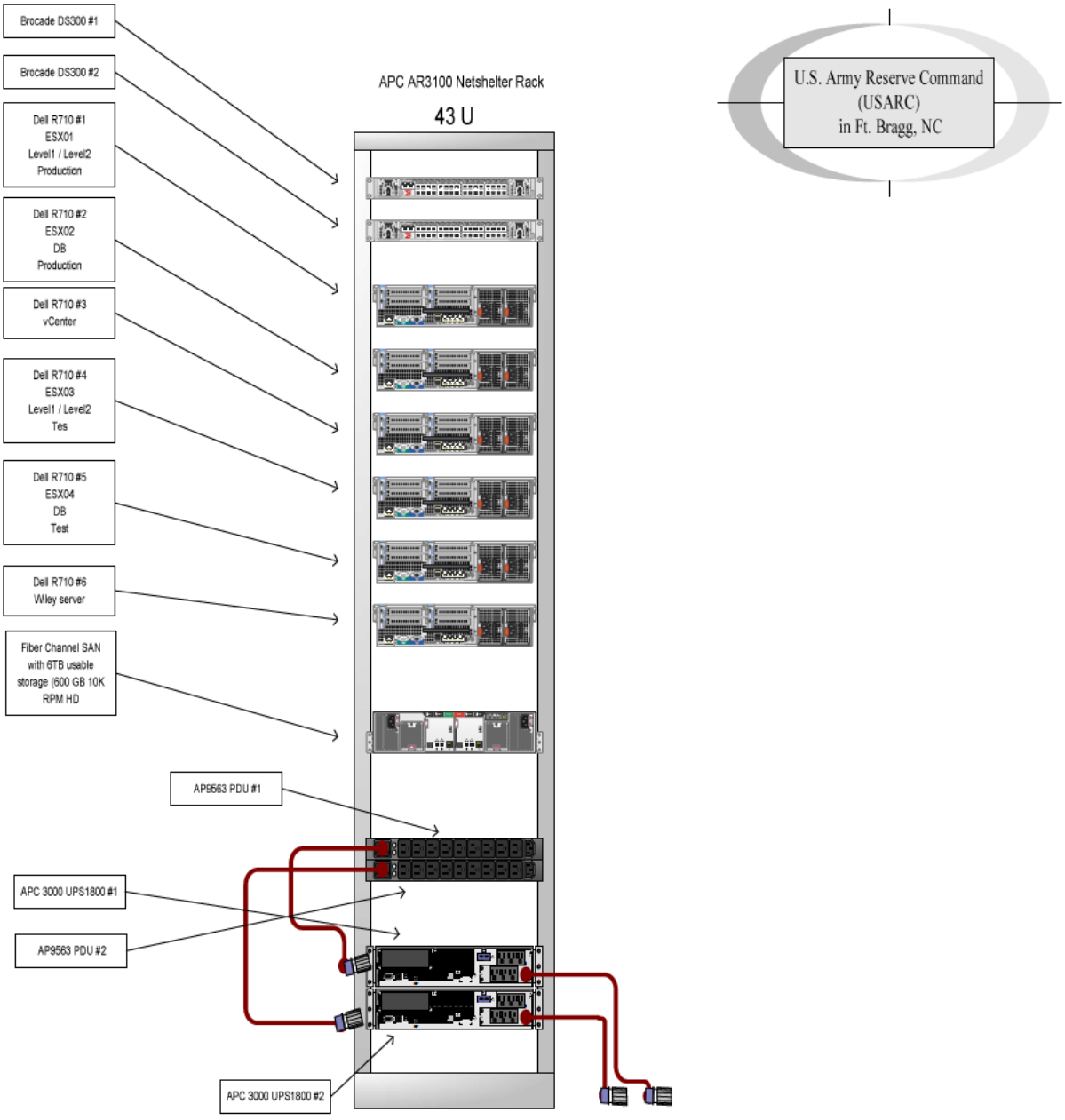


Figure 2. RCAS USARC Server Rack Diagram

Table 16. Rack Configuration (Bottom to Top)

Rack	Position	Make/Model
Uninterruptible Power Supply (UPS)	1-3 (3 Units)	American Power Conversion (APC) Smart-UPS 300XL
UPS	4-6 (3 Units)	APC Smart-UPS 300XL
SAN	7-12 (6 Units)	Hewlett Packard (HP) Storage Works EVA4400
RCAS Introscope CA/WILY Server	14-15 (2 Units)	Dell PowerEdge R710
RCAS Elastic Sky X (ESX) Host 4	16-17 (2 Units)	Dell PowerEdge R710
RCAS ESX Host 3	18-19 (2 Units)	Dell PowerEdge R710
RCAS V-Center Server	20-21 (2 Units)	Dell PowerEdge R710
KVM (Switch/Monitor/Keyboard)	23 (1 Unit)	Dell PowerEdge Rack Console 15FP
RCAS ESX Host 2 Server	24-25 (2 Units)	Dell PowerEdge R710
RCAS Production Database Virtual Instance	24-25 (VM on ESX Host 2)	Windows Server 2003 (VM)
RCAS ESX Host 1 Server	26-27 (2 Units)	Dell PowerEdge R710
RCAS Web Server (Level 1) Virtual Instance	26-27 (VM on ESX Host 1)	Windows Server 2003 (VM)
RCAS Web Server (Level 2) Virtual Instance	26-27 (VM on ESX Host 1)	Windows Server 2003 (VM)
SAN Fiber Switch Blue	38 (1 Unit)	HP Storage Works 8/24 Fiber Switch
SAN Fiber Switch Red	39 (1 Unit)	HP Storage Works 8/24 Fiber Switch
HP Network Switch	41 (1 Unit)	HP ProCurve 291 Oal 24G Switch

N.7 Maintenance Windows and Schedules

Release Updates Process:

Scheduled outages are conducted per the USARC Configuration Control Board (CCB) process for providing a 10-day notification in advance of the anticipated outage.

Routine Maintenance:

Regularly scheduled maintenance outages are set for Sundays. During this time period, updates are run and database cold backups are created along with any clones of the servers (as needed). Backups and clones are created in accordance with the RCAS Administrator Operations Manual (SOP/Maintenance). This is in the Fort Bragg, NC, DBA cubicle location: USARC HQ G-2/6 - Cubicle 2N2501-111.

Notification Roster In The Event Of an Incident:

- PI site Database Administrator/Systems Administrator/Site Manager
- E-mail sent to enosc_watch@usar.army.mil e-mail address which generates an enterprise wide unscheduled outage notification
- Applicable Product family leads
- Applicable Hardware Vendors if required
- Dell for Server Hardware
- PI Back Office team for Microsoft Operating System and Information Exchanges
- PI Database team for Oracle related issues
- Back Office and Database teams will contact third party software vendors as necessary
- PI Purchasing Manager if hardware needs to be replaced

APPENDIX O – FALLS CHURCH SERVICE DESK

O.1 Architecture

The Service Desk group has no mission critical servers or systems that they maintain. They rely upon the infrastructure team to restore all systems. In the event of short term service interruptions, personnel will implement applicable desktop procedures. In the event of long-term service interruptions, personnel have laptops available that allow for working remotely until service is restored. If the NGB Remedy Help Desk system goes down, there is currently no alternative solution as the Falls Church, VA Service Desk is a client of the NGB Remedy System.

O.2 Purpose

Enterprise Service Desk group handles the front facing customer relations. All AITS tickets are routed via NGB's Remedy system or the USARC Unicenter system to the enterprise service desk group. Tickets are then categorized and assigned to the appropriate product family or group for resolution.

O.3 Hours of Operation

Standard Mission Support hours are 0600-1700 Eastern Standard Time (EST) Monday – Friday.

O.4 Contact Information

- (b) (6)
- (b) (6)

O.5 Emergency Standard Operating Procedures

In the event of an emergency or natural disaster, AITS Service Desk team members (Section O.4) will contact their appropriate manager per the PI's policies via phone and email. If the event precludes personnel from reaching their physical work location, personnel will utilize laptops (stored at primary residences) that can access the NGB Remedy Help Desk system from alternate work locations.

APPENDIX P – USARC FORT BRAGG HELP DESK

P.1 Architecture

The RCAS USARC Fort Bragg Help Desk is comprised of two trouble ticket systems: Remedy-ARNG and Unicenter-USARC. In the event of short term service interruptions, personnel will implement applicable desktop procedures. In the event of long-term service interruptions, personnel have laptops available that allow for working remotely until service is restored. Responsibilities include verifying information and details pertaining to reported problems and ensuring that means exist to cross reference tickets that get escalated for support to Tier III.

P.2 Purpose

Provide full operation support to include system security, systems monitoring, troubleshooting, repair, performance evaluation, information exchange monitoring, and coordination between AITS Service Desk and the USARC service desk.

P.3 Hours of Operation

Standard Mission Support hours are 0800-1700 EST Monday – Friday. Critical Mission Support "Commercially Reasonable Effort" support after normal duty hours.

P.4 Contact Information

- (b) (6)
- (b) (6)
  (b) (6)

P.5 Emergency Standard Operating Procedures

In the event of an emergency or natural disaster, RCAS USARC Help Desk team members (Section P.4) will contact their appropriate manager per the PI's policies via phone and email. If the event precludes personnel from reaching their physical work location, personnel will utilize laptops (stored at primary residences) that can access the USARC network from alternate work locations.

APPENDIX Q – SUSTAINING ENGINEERS

Q.1 Architecture

The RCAS SE team consists of four engineers.

Q.2 Purpose

Provide onsite technical support for both ARNG and Reserve RCAS sites that require Tier II/III level support. SEs are also responsible for providing desk side level (onsite) assistance in support of trouble tickets. The RCAS SEs are also responsible for the operational support and maintenance of the Falls Church, VA, RCAS Training Servers and the RCAS COOP environment to include system security, systems monitoring, troubleshooting, repair, performance evaluation, applying RCAS updates and patches, creating student accounts for Soldiers attending RCAS functional training, and creating RCAS USARC user accounts if COOP has been activated.

Q.3 Hours of Operation

Standard Mission Support hours are 0800-1700 EST Monday – Friday.

Q.4 Contact Information

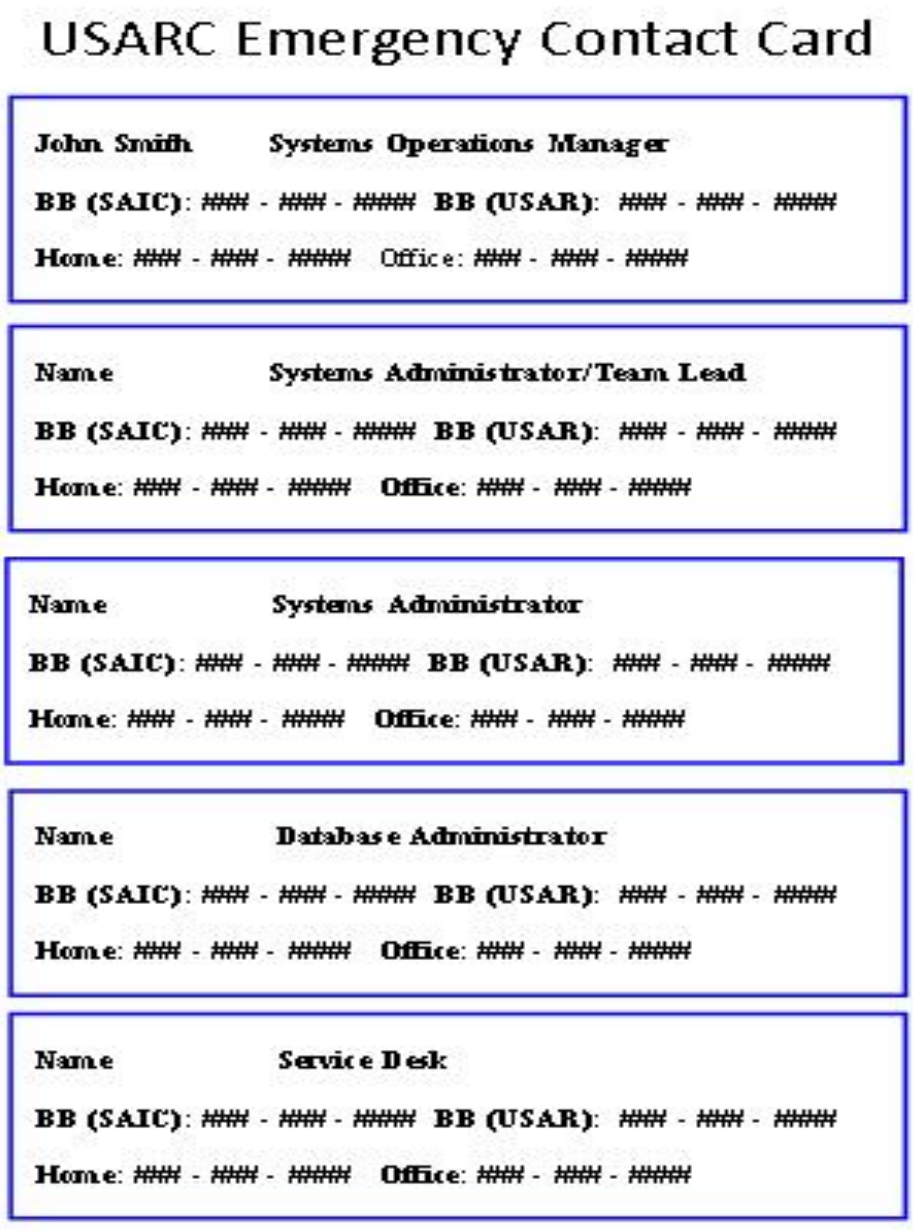
- (b) (6) [redacted]
- (b) (6) [redacted]

Q.5 Emergency Standard Operating Procedures

In the event of an emergency or natural disaster, RCAS SE team members will contact their appropriate manager per the PI's policies via phone and email. If the event is a service interruption, automated notification from the monitoring software could require SE support outside of normal working hours; all required personnel will respond. Hours will be adjusted accordingly to accommodate the situation and level of support needed. In the event of an emergency or natural disaster that precludes the RCAS SEs from reaching their physical work location, each member will attempt to establish contact via cell phones/BlackBerry devices or other available means. Each SE keeps available a set of RCAS release media and installation instructions (on CD/DVD) at their primary residences.

APPENDIX R – EMERGENCY CONTACT TEMPLATE – WALLET SIZE

Wallet template is for personnel with COOP responsibilities to utilize. Personnel can add applicable numbers and contact information as needed.



APPENDIX S – SAMPLE ANNUAL COOP TEST CHECKLIST

DEPARTMENT OF THE ARMY
OFFICE OF THE PROGRAM EXECUTIVE OFFICER
ENTERPRISE INFORMATION SYSTEMS
(PEO EIS)
9350 HALL ROAD
FORT BELVOIR, VIRGINIA 22060-5526

REPLY TO
ATTENTION OF

SFAE-PS

MEMORANDUM FOR

SUBJECT: Documentation of Annual Contingency Plan Test for [system name]

1. The FISMA Annual Contingency Plan Test for (PM/PD Name and system) was conducted on (DATE).

2. Contingency Plan testing is an important element of ensuring a viable contingency capability. Testing helps to identify problem areas and helps to evaluate the recovery staff to implement the plan quickly and effectively. The following areas were addressed in the contingency test:

Test Areas	Test Objective and Success Criteria	Results
1. System recovery on an alternate platform from backup media.		
2. Coordination among recovery teams. 3. Internal and external connectivity.		
4. System performance using alternate equipment.		
5. Restoration of normal operations.		
6. Notification Procedures.		

3. I acknowledge that PM/PD Name/System has satisfactorily met the Annual Contingency Plan Test Requirements (contingency test, after action review, final report completed) on Date.

IAM/IASO Signature Block

APPENDIX T – ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	Meaning
A&R	Authorization & Requirements
AGRMIS	Active Guard Reserve Management Information System
AKO	Army Knowledge Online
AITS	Advanced Information Technology Systems
APC	American Power Conversion
ARMS	Aviation Resource Management System
ARNG	Army National Guard
ARNG-IMS	Army National Guard Information Systems Division
ASCII	American Standard Code for Information Interchange
ASIP	Army Stationing and Installation Plan
BMO	Business Management Office
CA	Computer Associates
CD	Compact Disc
CM	Configuration Management
CMAS	Checklist Management Automated System
COOP	Continuity of Operations Plan
COR	Contracting Officer's Representative
CTP	Consent to Purchase
CWG	COOP Working Group
DARTS	Deployment and Reconstitution Tracking System
DB	Database
DBA	Database Administrator
DJMS	Defense Joint Military Pay System
DNS	Domain Name Service

Acronym/Abbreviation	Meaning
DTMS	Digital Training Management System
DVD	Digital Video Disc
ECRM	Enterprise Customer Relationship Manager
EI	External Interface
ENOSC	Enterprise Network Operations and Security Center
EST	Eastern Standard Time
ESX	Elastic Sky X
FATS	Field Accident Tablet System
FEDLOG	Federal Logistics Record
FM	Force Management
FOMSCOM	United States Army Forces Command
FTS	Full Time Support
GCCS-A	Global Command and Control System-Army
GUI	Graphical User Interface
HA	High Availability
HP	Hewlett Packard
HRC	High Resolution Converter
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilation, or Air Conditioning
IAPM	Information Assurance Program Manager
IAVA	Information Assurance Vulnerability Alert
IAW	In Accordance With
ID	Identification
IDB	Integrated Database
IDR	Integrated Data Reporting

Acronym/Abbreviation	Meaning
IE	Information Exchange
IP	Internet Protocol
JRMCB	Joint Risk Management Control Board
LIDB	Logistics Integrated Database
MEF	Mission Essential Functions
MOA	Memorandum of Agreement
MODS	Medical Operational Data System
MPDV	Mobilization Planning Data Viewer
N/A	Not Applicable
NGB	National Guard Bureau
O/S	Operating System
PBUS-E	Property Book Unit Supply-Enhanced
PD	Project Director
PD	Project Directorate
PI	Prime Integrator
PM	Project Manager
POC	Point of Contact
PROBE	Program Optimization and Budget Evaluation
RCAS	Reserve Component Automation Systems
RDS	Requirements Documentation System
RLAS	Regional Level Application System
MSC	Major Subordinate Command
SA	System Administrator
SAIC	Science Applications International Corporation
SAMAS	Structure and Manpower Allocation System

Acronym/Abbreviation	Meaning
SAN	Storage Area Network
SE	Sustaining Engineer
SFTP	Secured File Transfer Protocol
SLA	Service Level Agreement
SOH	Safety and Occupational Health
SOP	Standard Operating Procedure
STIG	Security Technical Implementation Guide
TAADS	The Army Authorization Documents System
TB	Terabyte
UPS	Uninterruptible Power Supply
USA PEO EIS	United States Army Program Executive Office Enterprise Information Systems
USAFMSA	United States Army Force Management Support Agency
USAR	United States Army Reserve
USARC	United States Army Reserve Command
VM	Virtual Machine
XML	Extensible Markup Language